Former Soviet Payphones!

This drab phone is a reflection of the monotonous life that awaits you in Kazakhstan.

Photo by William W. Perkins

This bright and colorful phone represents the constant fun and dancing that goes on every day in Kyrgyzstan.

Photo by William W. Perkins

Drabness returns to Armenia.

Photo by Derek Brown

Found in Belgium, easily the most mysterious and misunderstood of all the former Soviet Republics.

Photo by Vital Chaos

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Volume 15, Number 3
Fall 1998 $4.50 US, $5.50 CAN

2600

The Hacker Quarterly

"This is not a tool we should take seriously, or our customers should take seriously." - Edmund Muth of Microsoft, reacting to the release of Back Orifice, a program that attacks Windows 95/98 with a vengeance, by the Cult of the Dead Cow, as reported in the New York Times. We should point out that they said this BEFORE the program was released.

S T A F F

Editor-In-Chief • Emmanuel Goldstein

Layout • Ben Sherman

Cover Design • Bob Hardy, Crowley, The Chopping Block Inc.

Office Manager • Tampruf

Writers • Bernie S., Bitlsr, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Demeval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter.

Network Operations • Wicked, Izaac.

Broadcast Coordinator • Perkchop.

Webmasters • Fil, Kerry, Kratoy, Macki.

Voice Mail • Seju.

Inspirational Music • Electric Hellfire Club, Lionrock, Skinny Puppy.

Shout Outs • autojack, neka, Wilmington Waffle House, moja, foundation imaging, jason, michelle, doug thomas, nyc extramax protesters, lewis, micah, ct, alex, bruces, joel, states, winn, shipley, san diego 2600, phil hendrie & kfi, veggie, freqout, sdsc, jennifer, etherb.

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.

POSTMASTER: Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-1997 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $5.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com).

***2600* Office Line: 516-751-2600**
***2600* FAX Line: 516-474-2677.**

2600 Fall 1998

The Hacker Quarterly

provisions

progress

The summer of 98 was one of the most productive times we've seen in a while. And from the looks of it, it's just the start of yet another phase in whatever evolution we're going through.

We've said often that every time we get hit with something, whether it be word of a chilling raid somewhere, a masonic law that has no basis in reality, or something a lot closer to home, we wind up actually *gaining* strength when the dust clears.

Well, the dust is far from clearing but it's pretty obvious that we're heading someplace with renewed vigor. The hacker spirit is self-invigorating and it's surprising how many people either never realize this or forget it rather quickly as they move on in life.

Let's start with the close to home stuff. It was a year ago that we first told you about our crippling financial problems, caused primarily by our main distributors going bankrupt and taking a year's worth of our sales with them. We knew we weren't going to let this destroy all we've accomplished over the years but we felt we needed to explain why things might get sort of frozen and unhappy in the months ahead.

To the surprise of many, we didn't stagnate at all. Against the advise of everyone with a modicum of sense, we went forward with new issues, new projects, and new campaigns. We are eternally grateful to those of you who stuck with us in this difficult period, which, we are happy to say, is now behind us. Thanks to strong sales at the newsstands, we've been able to pay just about all of our printing debts and, by the time you read this, we should be entirely caught up. We lost a number of subscribers and we can certainly understand why. If there was even a remote possibility of our going under, who would want to lose their subscription payment? Now that we're back in force, we hope to see the subscription numbers go back up. The advantages to subscribing: you'll get your issues on time every quarter, you'll be able to take out marketplace ads for free, and you'll occasionally get extra things like the "Free Kevin" stickers we threw in with the Spring issue. We're not trying to discourage people from picking us up at the bookstores and newsstands but we feel it's important to also have a strong subscriber base in case we run into another distributor/bookstore catastrophe down the road.

While we lost a year financially, we were able to minimize our setbacks when it came to the truly important things. Since launching the "Free Kevin" campaign earlier this year, we've managed to raise nearly $3000 for Kevin Mitnick's defense fund through the sale of our bumper stickers. By revamping the www.kevinmitnick.com and www.2600.com sites, we were able to get many more people interested, and hence involved, in something that really mattered.

External forces deserve a lot of credit for moving us forward. The announcement of the *Takedown* movie in our last issue and in other forums produced a strong reaction, the likes of which we have not seen in our entire publishing history. It was bad enough knowing Kevin was still in prison after more than three years of waiting for a trial that never seemed to come. But now, a film that would portray him as a truly evil person and at the same time line the pockets of those who helped put him in the position he now faces? Even people who thought he was guilty of *something* came out strongly opposed to this.

It started in July with a demonstration outside Miramax offices in New York by around two dozen of us. That doesn't sound like much but whenever you can get that many people to stand in front of a building with picket signs in this day and age, it's a very significant statement. Sad but true. And the impact of that demonstration was clearly felt throughout the industry. Even the press took notice, although it took most of them a few weeks to get around to covering it. But in the end, our demonstration achieved everything it set out to do: raise awareness, begin a truly organized campaign, and show support for someone who was unable to defend themselves against a host of really powerful entities.

Miramax, to their credit, had the script rewritten several times, addressing nearly all of our objections to the original version. The infamous garbage can scene has been scrapped. Kevin is no longer portrayed as a violent racist. And, in a nod to reality, serious questions are raised as to just how involved Kevin actually was in the hacking of Tsutomu Shimomura's machine and, even more importantly, just why the FBI was targeting Kevin in the first place. But we can't say we support the film until Kevin himself feels that he's being treated fairly. As of this printing, that has still not happened.

We found a lot of the cause and effect we saw to be real inspiring. So much so that we decided to do something more. So, for a good part of the summer, a group of *2600* people drove through the entire country (unlimited mileage rental car) searching for answers in the whole Mitnick affair and filming as much of it as possible. We spoke with dozens of people on all levels of involvement in the case and came away with nearly 100 hours of footage. What we do with it now depends on what kind of editing equipment we can get our hands on but, suffice to say, we've got a fascinating story to tell and a most interesting counterpoint to the major motion picture that will be out in a year.

Considering the weakened state *2600* was in at the time we began this project, such an endeavor could best be described as foolhardy. Nevertheless, we knew this was the right time, and the only time, we could cover the story in this way. The "Free Kevin" movement has been growing with every passing month and the news of the *Takedown* movie only served as a catalyst. Again, good has come out of bad and all of us emerge from the darkness with more strength and determination.

We're certainly not the only ones getting the word out. All over the country, kids are handing out leaflets in their schools and malls, spreading awareness and adding to the movement. While we've heard many of them say they were inspired by *2600*, the real truth is that nothing makes all of this seem more worthwhile than hearing what they're doing. People in high schools and colleges are realizing they can make a difference, just by standing up for what they believe in. It seems like such a simple thing to do but so few of us actually take the trouble to go and do it. In the end, we believe this will be shown as one of the major reasons why the battle was won.

One of the most dramatic incidents in recent memory was the *New York Times* web page hack. On Sunday, September 13 (an extremely busy news day due to the Clinton scandal), hackers replaced the usual page with a rambling text, the entirety of which may have been hard for some to understand. But one section quite clearly told of the injustices of the Kevin Mitnick case as well as the culpability of the *Times* in his capture and the ensuing cashing in of the story. For many, this was their first exposure to any of this.

The message from Kevin and his attorney was very clear: this kind of thing is bad as it sends the wrong message and somehow makes it appear as if he's responsible for net chaos. However, we have mixed feelings. While doing something destructive in Kevin's name certainly won't help his case, we're not entirely sure that's what happened here. The *Times* is not claiming that there was any destruction to their original page. A

Progress Continued on Page 53

HOMEMADE TCP PACKETS

by Raff

The code presented here is a subset of my alpha perl spoofer, slapfro, which is available from 9mm.com/phlez.html. I thought it would be nice to see something other than a knockoff of a knockoff of a spoofer for once and maybe give some more people the ability to play with the insides of tcp/ip.

Greetz, boys and gullies. Today, we play with the insides of tcp/ip. In particular, we'll be building a tcp spoofer in perl (yeah, you can do icmp or udp too if ya want). We'll call this one - umm - lego. All we really want to do with lego is build our own packets. This can be useful if you like to set the source address to something arbitrary, or if you want to experiment with flags or some shit. We're not going to do tcp connection spoofing, because that would be too big in scope for our purposes. At this point we'll just send out some tcp packets with increasing port numbers, sort of like the way a half-openest portscan would look.

If lots of people begin to use this, we get the added benefit of making uptight sysadmins look silly, and finally teaching them that portscanning is neither harmful, intrusive, nor necessarily evidence that anything at all came from the apparent source of the scan. Ahem.

There are three main sections of code that we will use to create our packet: the first sets up things like source and destination address, ports, number of packets, and any looping and shit that we might use to send lots of packets or to vary the packets, say, by incrementing the destination port each time we send. The second section is the guts: we figure out what our ip and tcp headers will look like, then we put the packet together. The third section calculates a checksum for the packet - used to tell the receiving machine that the packet didn't get mangled in transit. I admit, I ripped off the checksum code from Net::Ping. Shit, who wants to write checksum code when it's already there for you? The three sections are nested 1,2,3 - they each use the next as a subroutine.

A Quick Tour

The first point of interest is the specifications of target box, source box, and ports. If your ambition is low and all you want to do is watch some borrowed tcp packets fly, just put in some valid source and destination addresses, run a sniffer, and enjoy. For the slightly more motivated, you could take these five items as parameters from the command line.

topspliff routine:

This is the first main routine - we do things like convert our hostname or ip address into something usable (gethostbyname) and set a few constants that we will use to indicate what we are building and how much of it we're responsible for (typically, the OS will do things like set the source address for you). We open our socket here and get ready to send the packet - we start the port incrementing loop, because we want to send one packet to each port in the range $dest_port_low -> $dest_port_hi. The only thing we need now is the packer. Our givehead routine, which used to be used only for headers, will construct the entire packet for us. At this point, we put no data in the packet (don't need any) but if you want to add some, just append it. Make sure you account for the increased packet length in your assorted length vars to come. Once we're done sending packets, we chill and have a 40, and our packet maker tells us that the scan is complete.

givehead routine:

This is the big baby Jesus routine of the program. I've taken the liberty of sticking literally *everything* in variables, so it will be hard to screw up. givehead does two things: first we create a tcp pseudo-header on which to calculate the tcp checksum. We do a lot of the setup of the tcp portion of the packet at this time, even though the ip header parts actually come first. We use the perl "pack" command to put each variable into the precise format that we need it in (see *ORA Programming Perl* for a reasonable but not great explanation of the pack statement). At this point, it would also be wicked handy to know what a tcp packet looks like - *get TCP/IP Illustrated Vol. 1*. It's the best. Otherwise you can browse the rfcs or find little charts from networking classes or something. Just understand the size, meaning, and ordering of all of the fields in a tcp packet.

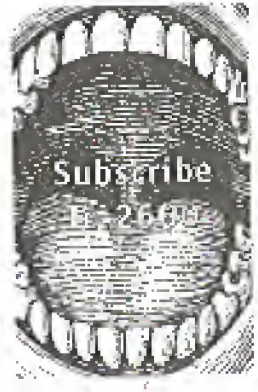
OK, enuff preachie. Here is where our more ambitious readers can really get loose. Take note of the $tcp_ variables, and later the ip_variables. Want to set a SYN, FIN, and RST in the same packet? Switch these to 1. Want to screw with sequence and acknowledgement numbers? Go ahead - even put in a little routine to increment them if you like. Make the packet length wicked long and send no data. Fool with the urgent flag and pointer (remember the OOB attack?), etc., etc.

Oh yeah - the second step, after we've got the tcp checksum, is to put it all together along with the ip header. This is a good place to set fragmentation options, type of service, time to live, even ip version. You should be able to build just about any tcp looking packet that you can imagine just by messing with the variables. Note to selves: do not put an unfriendly data type in a variable. Example: do not put a "2" in a bit field. Thanks for playing.

The last routine is the checksum routine, and, like I said, I stole it. (I re-commented it for aesthetic purposes). At least it ain't from guug.c.

Peace and enjoy.

[source on pages 8 and 9, built and tested on Slaux 2.0.28, perl v5.03]



lego source

article on pages 6 and 7

```
#!/usr/bin/perl
#
#  lego
#   tcp syn/fin dos proxy
#   written for 2600
#
#  based on slayfin, alpha version
#  written by w00f
#
#  TCP fake portscan only.
#
#  shout outs:  [illegible]
#

use Socket;
use strict qw(refs, subs);

#SOURCE AND DESINTATION PARAMETERS
# MUST CHANGE THESE.
my $target_box = "recipient.box.com";
my $target_low_port = "1";
my $target_hi_port = "20000";
my $source_box = "source.box.com";
my $source_starting_port = "10000";

tcsp00f($target_box,$target_low_port,$target_hi_port,$source_box,$source_starting_port);

sub tcsp00f  {
   my ($dest_host,$dest_port_low,$dest_port_hi,$src_host,$src_port) = @_;

   #set constants:
   my ($PROTO_RAW) = 255; # from /etc/protocols
   my ($PROTO_IP) = 0;  #ditto
   my ($IP_HDRINCL) = 1;  #we set the ip header, thanks

   #look up wth srit...
   $dest_host = (gethostbyname($dest_host))[4];
   $src_host = (gethostbyname($src_host))[4];

   #time to open a raw socket....
   socket(S, AF_INET, SOCK_RAW, $PROTO_RAW) || die $!;

   #now socket should be open...
   #now set the bad boy up...
   setsockopt(S, $PROTO_IP, $IP_HDRINCL, 1);

   my ($port) = $dest_port_low;

   print "\n INITIATING FAKE PORTSCAN \n\n";
   while ($port <= $dest_port_hi) {
          $src_port++;
          #build a tcp header.
          my ($packet) = givehead($src_host, $src_port, $dest_host, $port, $data);
          #sort out the destination...
          my ($dest) = pack('S n a4 x8', AF_INET, $port, $dest_host);
          #send a fuckinug packet
          send (S,$packet,0, $dest);
          $port++;
   }
   print "\n portscan sent, [illegible] \n\n ";

}

sub givehead {
   my ($src_host, $src_port, $dest_host, $dest_port, $data) = @_;

   #HERE WE PLAY WITH THE INNARDS OF THE TCP PIECE
   #AND CALC THE TCP HDR CHECKSUM.
   my $hdr_chksum = 0;  # we set it to 0 so we can calculate it
   my $zero = 0;  #might need a zero from time to time
   my $proto_tcp = 6;  # the protocol number for tcp
   my ($tcplength) = 20; # 20 byte tcp hdr; no data
   # IF YOU ADD DATA, MAKE SURE TO ADD ITS PACKED LENGTH
   # TO THE TCPLENGTH HERE!!!
   # all of the source and destination infos is passed to us
   # serve all it in the parent routine...
   my $syn = 79824563;  # random syn:  try to keep it under 32 bits :)
   my $ack = 0;  # zero ack:  try to keep it under 32 bits :)
   my $tcp_4bit_hdrlen = "5";  # 5 * 32bit (4 byte) = 20 bytes
   my $tcp_4bit_reserved = 0;  # reserved for 0
   my $hdr_n_reserved = $tcp_4bit_hdrlen . $tcp_4bit_reserved;  # pack them together
   my $tcp_urg_bit = 0;  # URGENT POINTER BIT
   my $tcp_ack_bit = 0;  # ACKNOWLEDGEMENT FIELD BIT
   my $tcp_psh_bit = 0;  # PUSH REQUEST BIT
   my $tcp_rst_bit = 0;  # RST (RESET CONNECTION) BIT
   my $tcp_syn_bit = 1;  # SYN FLAG BIT  #its a syn!!
   my $tcp_fin_bit = 0;  # FIN FLAG BIT
   # here we put together 2 reserved fields and the 6 flags to pack as binary.
   my $tcp_codebits = $zero . $zero . $tcp_urg_bit . $tcp_ack_bit . $tcp_psh_bit .
        $tcp_rst_bit . $tcp_syn_bit . $tcp_fin_bit;
   my $tcp_windowsize = 124;  # default window size
   my $tcp_urgent_pointer = 0;  # urgent pointer

   # the following is not a tcp header per se, but a pseudo header
   # used to calculate the tcp checksum.  yes, its a pain in the ass.
   my ($pseudo_tcp) = pack ('a4 a4 C C
                             n n n
                             N N
                             H2 B8
                             n v n',
                   $src_host,$dest_host,$zero,$proto_tcp,
                   $tcplength,$src_port,$dest_port,
                   $syn,$ack,
                   $hdr_n_reserved,$tcp_codebits,
                   $tcp_windowsize,$zero,$tcp_urgent_pointer);

   my ($tcp_chksum) = &checkfnv($pseudo_tcp);


   # PLAY WITH THE INNARDS OF THE IP PIECE HERE!!!
   my $ip_version = "4";  # (nibble) tcp/ip version number (current is 4)
   my $ip_hedlen = "5";  # (nibble) number of 32-bit words in ip header
   my $ver_n_hlen = $ip_version . $ip_hedlen; # we pack 2 nybbles together
   my $ip_tos = "00";  # (byte) ip type-of-service
   my ($totlength) = $tcplength + 20; #tcp + 20 byte ip hdr ##
   ## we'll pack totlength into 2 bytes in the packet
   my $ip_fragment_id = 31337;  # 2 bytes as well.
   my $ip_3bit_flags = "010"; # ip fragmentation flags (3 bits) (frag, do not frag)
   my $ip_13bit_fragoffset = "0000000000000";  #fragment offset
   my $ip_flags_n_frags = $ip_3bit_flags . $ip_13bit_fragoffset;
   my $ip_ttl = 64;  # 64 seconds / hops
   # we have proto_tcp from above...  my $proto_tcp = 6;
   # we have hdr_checksum from above...
   # all source and destination infos is passed to us (it
   #  gets set in parent routine)
   # change $syn and $ack above in tcp section
   # in fact, everything else in the packet is set above


   my ($hdr) = pack ('H2 H2 n n
                     B16 C2
                     n a4 a4
                     n n
                     N N
                     H2 B8
                     n v n',
          $ver_n_hlen, $ip_tos, $totlength, $ip_fragment_id,
          $ip_flags_n_frags,$ip_ttl, $proto_tcp,
          $hdr_chksum, $src_host, $dest_host,
          # end of ip header, begin tcp header
          $src_port, $dest_port,
          $syn,$ack,
          $hdr_n_reserved,$tcp_codebits,
          $tcp_windowsize,$tcp_chksum,$tcp_urgent_pointer);

   return $hdr;
}

sub checkfnv {
   #dis sekshun robbed from somewhere else....
   my (
       $msg            # The message to checkfnv
       ) = @_;
   my ($len_msg,       # Length of the message
       $num_short,     # The number of short words in the message
       $short,         # One short word
       $chk            # The checksum
       );

   $len_msg = length($msg);
   $num_short = $len_msg / 2;
   $chk = 0;
   foreach $short (unpack("S$num_short", $msg))
   {
       $chk += $short;
   }                                       # Add some less!
   $chk += unpack("C", substr($msg, $len_msg - 1, 1)) if $len_msg % 2;
   $chk = ($chk >> 16) + ($chk & 0xffff);        # bust out and [illegible]
   return(~(($chk >> 16) + $chk) & 0xffff);      # spray some chars
}
```

Socket Programming For Fun and Profit

by darknite
darknite@kuriz.net

First of all, this is no article for experts since I'm no expert myself on either TCP/IP or C. So all of those already familiar with the basics of socket programming may stop reading right now. And by the way, I am not responsible for any actions taken due to the information within this article. If you can't take responsibility for your own actions, what makes you think anyone else can? The reason for me writing this article was both to learn and to give some useful and creative information to all hackers/wannabes around the globe. Because even if every hacker doesn't write their own programs, they should be able to do so and understand the basics of them. Our goal in this article will be to create a portscanner. Simple and clean with just hostname lookup and no extra functions. This article assumes some basic C programming skills from the reader along with some basic knowledge and understanding of the TCP/IP protocol.

Finding The Host

First of all, we'll have to ask ourselves "How does a portscanner work?" The first thing a portscanner does is check the number of arguments given to the program. Since I suppose you all know how to do that in C I will skip the code for it. After that it will take the hostname, (argv[1]), to see if it's valid. We will use the gethostbyname(2) to process the given argument. (See code1)

```
code1:
struct hostent *host = gethostbyname(argv[1]);
```

The definition of hostent is found in <netdb.h>, (as is the definition for gethostbyname(2)), and looks like this:

```
/*
 * Structures returned by network data base library.  All addresses are
 * supplied in host order, and returned in network order (suitable for
 * use in system calls).
 */
struct  hostent {
        char    *h_name;        /* official name of host */
        char    **h_aliases;    /* alias list */
        int     h_addrtype;     /* host address type */
        int     h_length;       /* length of address */
        char    **h_addr_list;  /* list of addresses from name server */
#define h_addr  h_addr_list[0]  /* address, for backward compatibility */
};
```

This means that our IP number for the host given in argv[1] is stored in host->h_name. Let's write a little test program:

getip.c

```
#include <netdb.h>
void main(int argc, char **argv) {
  struct hostent *victim;
  if (argc<2) exit(printf("Use with host as argument.\n"));
  victim = gethostbyname(argv[1]);
  printf("%i.%i.%i.%i\n",victim->h_addr[0]
```



```
          ,victim->h_addr[1]
          ,victim->h_addr[2]
          ,victim->h_addr[3]);
}
```

As you can see, all four segments of the IP number are stored into a separate byte. So now we have the target host's address. What should we do next?

Establish Connections

A brief description of what really happens when you connect via TCP/IP to a remote host is in order.

First of all, you initiate a socket - let's call it "S". This socket allocates a free port on your computer. (It is the endpoint of the connection.) Once you have initiated a socket on your computer, you can tell that socket to connect to a port on a host. Let's say we would want to connect to the website at l0pht.com; here is what would happen (skipping nslookup).

Initialize socket S. (Got a free port, lets say you got 2222.)

Use S to connect to www.l0pht.com, port 80.

In theory your connection would look like:

S ---> www.l0pht.com:80

but in reality this is just:

yourhost 2222 ---> www.l0pht.com 80

So what we need to do is to create a socket and tell it where to connect. A portscanner connects to every port between a specified range on a host to see which ports (services) are opened and which ones are closed. Let's start to take a look at how to code this. To create the socket we will use the function socket(2). Here's the definition of socket(2):

int socket(int domain, int type, int protocol);

It returns an integer above zero (which is the socket handler) upon success or "-1" if it fails to create a socket.

Example usage of socket(2) is S=socket(AF_INET,SOCK_STREAM,0). The AF_INET is the ARPA internet protocol and the one we will use. The type we will be using is SOCK_STREAM which provides a two-way connection based byte stream. The protocol argument will not be used and is therefore set to 0, due to the fact that most of the times there only exists one protocol to support the particular socket type within the protocol family. The required header files for socket(2) and connect(2) is <sys/types.h> and <sys/socket.h>.

After the socket is created we will use the connect(2) to establish the connection to the target host. The definition for connect(2):

int connect(int sockfd, struct sockaddr *serv_addr, int addrlen);

sockfd is the socket descriptor/handler (S in our example). Instead of the sockaddr struct we will use the sockaddr_in struct, (so also include <netinet/in.h>) sockaddr_in looks like this:

```
/* Structure describing an Internet (IP) socket address.  */
#define __SOCK_SIZE__   16              /* sizeof(struct sockaddr)      */
struct sockaddr_in {
  short int          sin_family;       /* Address family               */
  unsigned short int sin_port;         /* Port number                  */
  struct in_addr     sin_addr;         /* Internet address             */
  /* Pad to size of `struct sockaddr'.  */
  unsigned char      __pad[__SOCK_SIZE__ - sizeof(short int) -
                     sizeof(unsigned short int) - sizeof(struct in_addr)];
};

struct in_addr {
        __u32   s_addr;
};
```

By what you can see above, the sin_addr.s_addr is just an unsigned 32 bit number to represent the

IP number (for example 0x7F000001 is 127.0.0.1). So how do we convert the result in host->h_addr given by gethostbyname(3)? Easy, we'll just cast the host->h_addr with *(long *)(host->h_addr). Finally, don't forget to use the htons(3) to convert it to revers byte order on x86. And the addrlen argument is just sizeof(sockaddr). We will have to cast our sockaddr_in variable to a sockaddr struct when passing it to connect(2). And of course, one final thing, don't forget to close down your socket. Use close(2) with your socket as argument. Like: close(s) (The definition of close(2) is found in <unistd.h>.)

Writing The Code

New when your fingertips are itching to get down to business don't let me hold you back. You should without problem be able to write a portscanner or anything else - only your imagination sets the limit. No guide is complete without that final piece of source code, so here it is:

```
portscan.c

#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <netinet/in.h>

#define START 1
#define STOP  1024

void main(int argc, char **argv) {
  int s,port;
  struct hostent *host;
  struct sockaddr_in victim;

  printf("PortScan v1.0 - By darkrite[@kurir.net]\n");
  printf("for his socket-programming article in 1998\n");
  if (argc<2) exit(printf("Usage: %s <hostname>\n",argv[0]));

  host=gethostbyname(argv[1]);
  if (!host) exit(printf("Error looking up hostname.\n"));

  victim.sin_family=AF_INET;
  victim.sin_addr.s_addr=*(long *)(host->h_addr);

  for (port=START; port<=STOP; port++) {
    victim.sin_port=htons(port);
    s=socket(AF_INET,SOCK_STREAM,0);
    if (s<0) exit(printf("Error creating socket.\n"));

    if (!connect(s,(struct sockaddr *)&victim,sizeof(victim)))
      printf("port: %i\n",port);
    if (close(s)) exit(printf("Error closing socket.\n"));
  }
}
```

As I have said before, I am no expert on socket programming nor TCP/IP communication. But I believe this should be enough for anyone to get started with socket programming and to write some handy tools. Since I only use Linux, everything in this article has been tested under Linux only, but I believe that it should work fine on all other UN*X systems too. (You might have noticed that when introducing a new function I have included the man section number for that function - use man as frequently as possible.)

Good luck with your programming.

Blasting Sound

by Slatan

I have had so much fun with this little program. The first time I used it, it was truly amazing. I almost pissed, I laughed so hard. What this program does is exploit the fact that some Unix's (running Novell on hp's) don't require you to remotely log into another computer to send them a sound. So as soon as I learned this, the wheels started spinning. OK, I was thinking, let's see what I can do to exploit this. No sooner had I asked myself this than it hit me. This network isn't really laggy, I wonder how long it would take for me to send a sound to each of the workstations. So I wrote this little program to see. First what you need to do is make a list of all the computer names hooked into your network. Call it list. You also need the program called send_sound, which is installed by the defaulted software on these workstations, so do a search for it. Place it in the same directory along with the sound files you wish to use.

For my first sound I sent a short zap sound. I think I got it from a laser blast somewhere. Oh man, was that funny. It hit every computer so fast - everyone stood up and looked around as the sound went from computer to computer, then row to row. It sounded like the Fourth of July in there.

For my next sound, I felt like hearing some applause for my efforts, so I sent a round of applause, which turned out to sound like a rock concert inside there. By this time the supervisors were very curious to see who was interrupting the workday. Haha.

By manipulating the file list I could have the zap sound bounce around the large building I was in, which was fun too. Be creative - annoy your neighbors and friends!

```
#This program is for blasting sounds at people that annoy you
#Use and abuse!
#Hacked Cracked and Coded by --H8RED-- aka SLATAN

#To use this program you must have the program send_sound and the
#sounds you want to send in the same
#directory together.  Change the $HOME/"to where this program is
#located" next create a list called "list",
#in the same directory and put the tube number or numbers you wish to
#blast  Ex: computer715 or whatever the other computer's name is.
#then run this program and tab down to the argument
#box and type in the sound you wish to send Ex: zap.au
#hit okay and bam! you blasted them.

#/*************************************************************************
#/*  Program ID  : SoundBlaster                                           *
#/*  Description : This program is used to Blast the hell out of people   *
#/*  Input Parameters : Type in the sound name next to argument           *
#/*  Exit Value       : None                                              *
#/*  Input Files      : Must have a file called list in the same directory *
#/*                     as this program                                   *
#/*  Output Files     : Creates a file called USERS                      *
#/*  Link Procedures  : None                                              *
#/*  Special Logic    : None                                              *
#/*************************************************************************
#/*              M O D I F I C A T I O N   L O G                          *
#/*   Date          Author                 Description                    *
#/*  ----  ----------  -------------------                                *
#/*  04/25/97  --H8RED--             Initial Release                      *
#/*************************************************************************

#!/bin/ksh

for node in `cat list`
do
echo '----------------------'
  echo Snode # `date`
 $HOME/send_sound -server $node $1 $2 $3 $4 $5


done
```

BACK ORIFICE TUTORIAL

by skwp

The hacker group known as Cult of the Dead Cow (CdC) recently released a great hacking tool known as Back Orifice, or BO, on August 1, 1998. On August 9th the client code was ported to UNIX. The legitimate purpose of BO is the remote administration of one's machine. BO affects Win95/98 but not NT. The following article explains the uses of BO, how it works, and how to prevent it from attacking you. Much of this information is taken from BO documentation and resources on the net.

How It Works

BO consists of two parts, a client and a server. You have to install the server on the machine you wish to gain access to. The server is included in the BO installation as beserver.exe. Once run, it self-installs, and then erases itself. After that the server machine will run BO server every time it starts up. The process is not visible in the processes list (ctrl-alt-del) The server exec itself copies itself to c:\windows\system as "<random>.exe".

The server can be configured using beconfig.exe, which allows you to specify the name of the file (default: "<random>.exe"), description in registry, port (default: 31337), and password (default: no password) among other things.

Once the server is installed, you can use boclient.exe (bomix for the unix versions), or bogui.exe (graphical) to access the server machine. The client sends encrypted UDP (connectionless) packets to the server machine in order to communicate.

How To Get It Installed

Here's where our favorite skill, social engineering, comes in. Make up any kind of bullshit story in order to get the person to run this file. Pretend to be a friend, say it is a new game, tell them it's a couple of xxx pics in self extracting format. Be original, and don't push them to run the file - this will make people suspicious. When they run it they may say something like "What the fuck? It disappeared." This is when you know that you have full access to their machine.

Using the Client

The client interface has many features. You can read the supplied docs. I will discuss some of the more fun features and their uses.

Once you start the client you can type "help" or "?" for assistance on available commands. First of all to connect to a machine you have BO'ed, use "host <ip>".

Now you can use standard DOS commands (dir, cd, copy, del, etc) to move around on this person's hard drive. However, this is awkward and takes a long time. Luckily, BO includes a built in http server so that you can download and upload files to the machine. Use "httpon <port#>" to activate the http server. Now you can access their machine through a web browser on that port (I use netscape: my friend reports weird problems accessing BO'ed machines while using Internet Exploiter.) BO includes a convenient form on the bottom of the page for you to upload files. Fun things to do while browsing: look at person's pr0n, read personal docs, steal warez.

Another fun thing to do, which tends to scare the shit out of people, is to display a dialog box on their computer. Use "dialog <text> <title>" to make a dialog box pop up on their machine. I have found that in the windows boclient, the dialogs do not come out right if you use quotes. I'm not sure about the linux version as I have not been able to test it. However, using the gui client for windows this bug does not exist. Be careful using this as it lets people know that their machine is in the process of being owned and they tend to reboot as quickly as possible. If this happens you can use the sweep command to sweep their subnet and find their machine again (in the case of dynamic ip's). You can also use the multimedia "sound" feature to play sounds on their machine. Specify the full path to the sound.

The network commands menu allows you to view their network and share resources. This may prove to be very fun. Share their printer and print out a nice message telling them how to remove BO (discussed later).

You can also have fun with processes. Use "proclist" to list running processes, and "prockill" and "procspawn" to kill and spawn new processes, respectively. This is useful, for example, if you have modified some sort of ini files (like mIRC) and you need them to revert the program. Just kill the program and they will probably revert it, thinking it was just a stupid windows bug.

One of the more fun features of BO is keystroke logging. This feature will log all keystrokes in a very convenient manner, including the name of the window where they were typed, into a text file on the person's machine. Use the http server to download/view this file. Another convenient way to get passwords is the "passes" command which lists cached passwords. I have found many unencrypted passwords sitting around in this way, including passwords to Tripod homepages and PPP accounts.

Finally, you can redirect ports and tie console apps to ports. For example, if this person is running a 31337 WaReZ FTP SeRvEr, you may want to redirect all connections to port 21 to pentagon.mil, or whitehouse.gov. I can only think of one example of tying apps to ports which is included in BO, and that is to tie command.com so that you have a DOS shell on their machine. Usually you can just put it on port 23 (default telnet port) which makes it a lot easier. I have found, however, that accessing their machine in this way is extremely slow for some reason.

Other features of BO include modifying the registry, capturing screenshots and movies from attached input devices, and using plug-ins (read included plug-in docs for info on how to write them), locking up the machine, and rebooting it.

BO and plugins (bopluglns) can be downloaded at:
http://www.cultdeadcow.com/tools/

How To Get Rid Of It

According to the ISS Security Alert Advisory made on August 6, BO installs itself by entering itself into the registry. To stop BO from starting every time the machine boots, edit the key at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices and look for any suspicious program names. The length of the BO exe is close to 124,928 bytes, give or take 30 bytes. Erase this entry, and erase the file itself. If possible, format your hard drive and reinstall all OS's and software, as the use of BO may be part of a larger security breach. The full text of the ISS Advisory can be found at:
http://www.iss.net/xforce/alerts/advise5.html

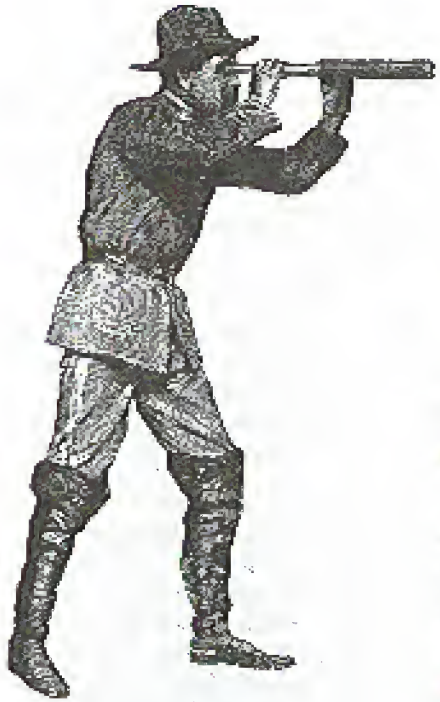
Microsoft's Response

"This is not a tool we should take seriously, or our customers should take seriously..." - Edmund Mush of Microsoft, as reported by the New York Times.

Well, Microsoft was wrong. There have been an estimated 65,000 downloads of the BO software package, and I myself have owned over 15 machines using it (I was bored, wanted to look at other people's pr0n....).

Conclusion

Back Orifice is a fun toy, but you must remember hacker ethics while using this tool. Do not put something like "@echo y | format c:" in autoexec.bat. The purpose of hacking is to learn and create, not to destroy.



Probing Remote Networks

by Armageddon

Let's just say I decided to investigate a network, something.net, for one reason or another. It could have been for any reason - it doesn't matter because if I told you it might give away what network I was investigating.

Anyhow, I just left ws ping propack (http://www.ipswitch.com) on all night to scan the subnet and scanned up through ports 1024. I came back in the morning and guess what turned up? Basically, port 23 was open on almost every machine. Port 53 was open on the two name servers (duh). Port 21 was open on a few machines. Ports 110 and 25 on mail.something.net were open (that was a given).

The first thing I did was telnet to port 23 on host1.something.net. It established a TCP connection, but then it disconnected me. I figured it was either a firewall or the machine I tried to telnet to would only allow connections if I was a trusted client. Either way, that is a hitch to work around. So what next? I started scanning for ports on which I was able to maintain my TCP connection. I found that every port but 23 would let me maintain a TCP connection. Talk about lax in security. I figured they thought if they didn't allow port 23 connections they didn't have to worry about people logging in. Which is pretty stupid.

So I figure this would be an easy hack. Anyhow, most of the machines on the network were SunOS 5.5.1. Some freebsd machines were also on the network (lucky for me I like freebsd). I started looking around for any exploit I could find without much luck. So I figured out the freebsd machine was version 2.1.6. That machine was a little outdated; they must have just kinda forgotten about it or something. So I decided to pick on it, because it might have just been the one weak link in the chain I needed. A portscan returned ports 7 (echo), 23 (telnet), 25 (sendmail), 53 (dns), 79 (finger), 80 (http), 111 (sunrpc), and 513 (remote login). Anyhow, the first thing I always think of is sendmail, and I remembered that freebsd was shipped with a vulnerable version. So I telnetted to port 25, and... it's 8.8.8. Damn, that door got slammed in my face.

So next I looked at port 53, the name server. I believed that it was the secondary name server because its OS wasn't that up to date. In an attempt to figure out where exactly the name server was placed I did a traceroute to it. Then I ran a traceroute to a few other computers. The result: each traceroute turned up cisco-7k.something.net. I am gonna bet that that is a Cisco 7000 router (some nice hardware). On the last two computers where I ran a traceroute was anyname.something.net. I believe that to be a firewall because almost all traceroutes pass through that computer, and it appears just after the router. But it didn't appear when I did a traceroute to what I believed was the secondary domain name server. So then I decided to do a whois something.net and found what the two name servers were (why didn't I think of this before): ns1.something.net and ns2.something.net and of course the outdated freebsd machine was ns2.something.net. All right, I'm in business.

I then ran a traceroute to ns1.something.net and it didn't pass through the firewall, which meant that they had their name servers set up outside of the firewall. (It's very typical to put name servers in front of the firewall.) So I searched the sploit archives for a freebsd exploit, and a named exploit came up - talk about my lucky day. So I compiled and ran it. I then got myself a root shell on the name server. (No, I will not give you the source of the exploit; that would be aiding you in attacking a computer). Too bad it was outside the firewall.

So was there anything of any use to me? Yes, of course. The master.passwd but it's only good I imagine if they are running NIS or NIS+. So I issued the ftp command back to some computer on the Internet (not my computer, that would be stupid) and downloaded it. Eventually I got it back to my computer. I started good old John The Ripper right away and continued to explore the network because what good is a username/password if you can't get in because of a fucking firewall?

Anyhow, on one machine I found an anonymous ftp server. So I decided to check it out, and I found that the machine was running SunOS 5.5.1, and it was vulnerable to an ftp bounce attack! Hell yeah. So now I went and grabbed that script and ran the little devil; it bounced me straight through the anonymous ftp and to a telnet port on the subnet. Now all I had to do was crack that password file. So I waited a long while as John The Ripper went to town, day and night on the password file. Then finally I just took the first login I got, and boom, I was on this system which was inside a firewall! Hell yeah!

So I had to get root. Would su work? If it did, kickass, but if it didn't I may have been screwed. Since I always play it safe, I looked for something I could run on the shell to get me root. Now that I had passed the firewall, I could just use any remote buffer overflow and get root on any of the computers. Or, I could just log into another system anywhere and run a local root exploit. I had a wide range of exploits to choose from.

I figured I'd look around and see if I could find another freebsd machine lying around to screw with and bam! freebsd 2.2.1. This one had a local root exploit in the /proc filesystem. I got the list of username/passwords and I was past the firewall so I figured this would be pretty simple. I telnetted over to the freebsd 2.2.1 box, and ftp'd the exploit source over, compiled the thing, ran it, waited a few minutes, and bam, root shell!

Anyhow, I searched around the network for what I came for and ran those nifty little cloaking programs to cover my ass. I wiped all the necessary logs to hide my presence and got out. It was rather daring to jump around to so many machines, but since I only came for one reason and got what I needed, I didn't leave any backdoors for myself. And I didn't change anything. So I should get off scot-free.

HACK YOUR CONSOLE

by m0rion

You may be saying to yourself, "Hack your console? You mean, like my Nintendo64?" If you've never heard of it, yes, you can "hack" your console. This is not your traditional "hacking" as far as getting into systems by cracking passwords, but rather, using your console as it was not meant to be used.

First off, let me start by saying that I think the idea of consoles is great, obviously not as good as computers, but great nonetheless. I also think the games are overpriced ($60 for a game it costs them $5 to make? Get real...) and many people agree. There are ways to take your Nintendo64 and turn it into the *real* ultimate fun machine, especially for you programmers out there.

Back-up Devices

You see, these super little inventions called "back-up devices" have been invented for the Nintendo64. And they do, much as the name suggests, back-up games. You can take a game, and copy the ROM image and SRAM image to a form of media (varies from each back-up device). This is so that if your cartridge is damaged or broken, or you accidentally delete a saved game, you have a ready back-up of such things and don't have to spend money on a new one.

These back-up devices are mainly made in mainland China and are imported to the US or Canada for sale. You may also see them mentioned in the back of Nintendo's game manuals stating that they are illegal and you will be prosecuted if you use one. But, make no mistake, the right to back-up your own electronic information is *perfectly* legal. Reasons why Nintendo *still* tries to convince people they're illegal are unknown.

Other Uses

Here is where the real legal issues come in. If you back-up a rented game, or a friend's Nintendo game and keep the ROM, you are committing piracy. This also applies to those of you who may download ROMs over the internet (many FTP and HTTP sites offer this).

However, yes, it is possible (and very easy) to download or back-up ROMs from friends and play them for "free" on such back-up devices. So, basically, if you're willing to live with committing a crime (and you'll probably never get caught), you can buy a back-up device and download every game for the Nintendo64 and play them freely.

Also, and here is the *real* good part, you can program for the Nintendo64 and play the games you've programmed or upload them to sites on the Internet for others to play. There are many SDKs full of image and object libraries available on the Internet for the Nintendo64. Such devices similar (almost identical) to the back-up devices are available from Nintendo Inc. for up to $40,000.

Types of Back-up Devices

There are basically three mainstream (if you can call them that) back-up devices. I will go through the names and descriptions one at a time.

Mr. Backup (Z64) - This is the back-up device I own (and probably the most favored). It loads on top of the Nintendo64 in the cartridge slot and has a slot on the side of the device for a cartridge to be inserted. On the right side of the device there is an Iomega Zip drive for inserting Zip disks. And finally on the top of the device there is an LCD display which gives options and shows the ROM contents of the Zip disk.

This device runs off of a 386 SX/40 and has a flashable BIOS chip. It runs off a 5v power supply and also has an option to connect a CD-ROM or SyQuest Syquy drive to the inside, although these have to be powered externally. The Zip drive is connected through regular IDE cables.

Doctor64 (V64) - This is a very good back-up device, although not as versatile as the Z64. It comes with a CD-ROM and loads on the bottom of the Nintendo64 (in the EXT slot). Its BIOS displays onscreen (also flashable) and has options and also shows the ROM contents of the CD. Now, you cannot back-up directly onto the CD, obviously, so you must connect it via Parallel Port to a computer and the ROM image must be transferred to the hard drive. You can then burn ROMs to a CD for use. This device also supports Audio CD play and VCD (Video CD) play. Recently they started supporting MPEG-1.

CD64 - This device is *very* similar to the V64. It uses a CD-ROM also and has all the options of the V64 (including parallel port). However this does *not* support audio CD, VCD, or MPEG-1 play. Not necessarily a large disadvantage, but a disadvantage nonetheless. This also loads through the bottom of the Nintendo64.

Where? How Much?

These back-up devices are widely available over the Internet (in fact they're not available much anywhere else). The Z64 will run you about $350 and can be ordered at www.z64.com. The V64 is about $280 and can be ordered at www.carlind.com. The CD64 will run you about $180 and is available at www.cd64.com. There are also NES, GameBoy, and Super NES back-up devices available which are similar to those above except they take 3.5" floppy disks. They are available along with some other cool console stuff at:
http://surf.to/vividbarrier

Additional information about all N64 systems is available at www.dextrose.com. I highly suggest you take a look at this page for more information before you order. You can also talk to many people who own such devices (and sometimes people from the companies above) on IRC. Just go to #n64roms on EFNet.

Final Notes

Some additional notes about system RAM. The way the ROM is played it is loaded from the media onto system RAM. Currently there are three image sizes for the N64 which are 64 megabit, 96 megabit, and 128 megabit. Remember, 128 megabit is equal to 16 megabyte (megabyte is probably the term you're more familiar with, it's what your hard drive is measured in) and all systems ship with 16 megabytes of RAM which supports all games. However, new games coming out are up to 256 megabit (32 megabyte) which would require an upgrade to 32 megabytes of RAM. All systems have this ability and if you wish to program games that range about 128 megabit, you must also upgrade your RAM.

Programming note: you are *not* limited to 64 megabit, 96 megabit, or 128 megabit. Your program for the N64 can be *any size* as long as you have enough RAM to support it.

Ordering notes: all the companies listed above are completely legitimate. However, I have heard of shady companies out there that try to rip you off. I would suggest checking the companies out before you order from them. I have done business with the companies above and have had no problem with service from them.

Once again I'd like to state that copying games is illegal but backing up is not. I know many people who have bought these systems for the purpose of copying games and it has worked *perfectly* with every game, but this doesn't make it "legal." It's basically your call whether you want to break the law or not.

CUSHIONED ENCRYPTION AND DENIABILITY

By Phunda Mental

As I'm sure most of us know by now, the world is getting to be a scary place. We are getting placed in bondage against our wills when there is little or no evidence that any crime was committed, or that anyone (other than the Feds' sense of order) was somehow harmed.

With the latest examples of injustice, such as those endured by Bernie S. and Kevin Mitnick, it is no stretch of the imagination to envision a case in which a person is held in prison for failing to reveal her encryption key. Certainly a warrant can be legally obtained for such a key, and this makes sense when we understand cryptography merely as a way to lock away secrets. The problem with this model is that the very same bits that serve us as locks also serve us as identification. If a law enforcement officer obtains the keys to our files, he can also "prove" to our associates that "he is us." He can sign digital contracts in our names, and even sign digital confessions for us. A scary proposition.

It is for these reasons that I began looking for a way to pull one over on Joe Officer. Simply hoping against hope that the government will keep itself away from our keys is probably naive.

What we would like to have is a system where if Joe Officer demands the key to our ciphertext file, we can choose to supply one of many keys. One key might reveal a love letter to his wife, the other might reveal the completed works of Shakespeare. A third key might give us our secret documents. This is usually called deniable encryption. This term usually carries the added stipulation that user be able to invent keys on the fly, when pressure is applied by enforcement to reveal a meaningful text. I don't find this idea to be that great though because this assumes that the decryption is done in a black box; in other words that law enforcement isn't watching us and looking at our programs. They would see us invent a key for a given plaintext.

Instead of this, I find it preferable to decide beforehand what plaintexts will be available. In this way, law enforcement sees us apply a key with a given algorithm, the plaintext simply appears out of that. No specialized calculations specifically for deniability need to take place. The enemy would know that we probably have a means to extract other data sets, but any additional data in there can legitimately be said to exist to frustrate cryptanalysis, in the terms we will use, this data is just junk chaff. I call this type of system a "cushioned" encryption system, that is, we set up an alibi to fall back on beforehand. But before we consider this method, let's look at the simplest method of deniability.

The most obvious way to achieve this is with a one-time pad. An OTP has the property that a key can be constructed to reveal any possible message of length N from ciphertext (also of length N). To achieve this feat, however, our key also needs to be N bytes in length. This might be OK for a few bytes here and there that we can remember the pad (key) for, but in this case why not just memorize the plaintext and be done with it?

We can store all of the pads on disk, but not only is this troublesome to work with, Joe Officer can simply confiscate all of the pads. Even if the pads are encrypted with PGP, he just demands the key to the pads instead of to our secret document.

One-time pads just aren't going to cut it.

Enter Ron Rivest. Rivest, most widely known for his work on the RSA public key algorithm, recently introduced a small paper on a method of data confidentiality that he calls "winnowing and chaffing."

The basic w/c method is discussed in [RIV98] and is a really interesting idea. Rivest proposed it as a method of achieving confidentiality without encryption: the plaintext is transmitted in the clear. See Rivest's paper for how this is done – if the material in this article is not clear, read Rivest's paper to get a clear understanding of the basis of w/c, and this stuff should fall right into line with you.

For our purposes, what we want to look at is merely the idea of using MACs (Message Authentication Codes) to separate one strand of data from another.

What we are going to do to achieve our goal of deniable encryption is to use two tools: a strong hash function (H) and a symmetric cipher (C). Of course, we can turn any hash function into a block cipher and vice versa, so we could really do it with one tool, but that is academic.

We need a passphrase from the user, which gets hashed with H() like so (the notation gets a little slippery, but stick with me):

H(user_passphrase) → k

H(user_passphrase+k) → k' where + denotes concatenation.

It should be noted here that H() may be something like SHA-1 or MD5, but it would be preferable to use a complete MAC system like HMAC. For our uses here, I believe that ordinary hash functions will suffice. However since HMAC is available in good crypto libs right next to RC4 (for our byte by byte encryption, RC4 is the easiest to implement and block ciphers offer no obvious advantages to a stream cipher with just heavy MACing), so all the tools are right there for you, use HMAC.

But let's get back to the algorithm:

k is the key that we will use for our cipher, and k' is the key that we will use for MACing. For every byte of plaintext that we get, we will also increment a sequence number (sqn). "+" denotes concatenation.

1. We grab a byte of plaintext (P)
2. Encrypt: C(P,k) → M #encrypt P with k yielding M
3. MAC: H(M+k'+sqn) → M' #hash M, k' and the sequence number together
4. Output M | M'
5. If we have more bytes, goto 1.

To decrypt this stuff, we do the following after we get the user's key and set up k and k' as before. D() denotes the inverse of C().

1. Grab a block of data, and separate out M and M'
2. H(M+k'+sqn) → R' #recalculate what we think M' should be and call it R'
3. If R' and M' match, decrypt M, D(M,k) → P
4. Output P
5. If we have more bytes, goto 1.

To see how this lets us form deniable encryption, imagine what would happen if R' and M' did not match in the decryption process. We simply discard that packet and move on. Rivest calls this winnowing. Why wouldn't M' and R' match? Because M' was created with a key different from what the user supplied in the decryption process. That packet may very well be meaningful data, it was just encrypted with a different key. This allows us to encrypt two or more files using the ciphertext of each file as chaff for the others. An example is in order.

Let's define two messages that we want to send, the bytes "A" and "B." The keys for A are k=S, k'=T and the keys for B are k=Y and k'=Z. We start our sequence number at 1.

Let's suppose that our functions H() and C() do the following:

C("A",S) = G – M = A "A", encrypted with key k (= "S") yields "G"

H("GS1") = "2" = M' # hash the ciphertext byte above with k' and the sequence number, yielding 2. This is M'

So our first message packet is "G2" - on to the first byte of the second message:

C("B",Y) = O # "B", encrypted with key k (= "Y") yields "O"

H("O7.1") = "8" = M' # first byte of the second message, use 1 for sqn

Ciphertext output (both messages merged and interpolated): G2O8

When we attempt to decrypt the first block of our message we have some keys that the user supplied. If the user supplied k=S and k'=T then we will accept G as a valid byte (M' and our calculated R' will match) and we reject O: we have just stripped out the second message's byte leaving only the first. Now we can just pass this byte through D() which will yield the plain text, in our case "A." If we supplied the other set of keys (k=Y and k'=Z) then we would have stripped out A and decrypted O and therefore obtained B.

It is easy to see how this can be used against Joe Officer: if he wants A we hand him the keys to B, if he wants B we hand him the keys to A.

To round out the method and make it all hold up, we insert chaf packets (just some random bytes that won't be accepted by the MACing) at random intervals. If scrutinized, an attacker will have no idea whether or not the packet in question is a bogus chaf packet or a meaningful packet. There is no obvious analytical way for an attacker to show whether more meaningful data exists in the file or if the contents are just random bytes. The most "straightforward" way of attacking this system is to dictionary attack the user passphrase, as always. Failing this, one must attack the hash function and the cipher. This gets difficult very quickly.

Another modification to this basic system is to obtain more data from the user's passphrase through multiple hashes and using this additional data to seed a cryptographically strong PRNG and grabbing 128 bits or so from the PRNG and hashing this into each MAC. This ensures that there is always a good amount of new bits getting turned over to the hash function. If the hash function is biased, this bias may be able to be used to predict how the digest bits change in the next hash, the sequence number is incremented, so the changes in these bits are also minimal. The remaining bits are just those 8 bits for the plaintext byte. Known plaintext statistics can be used here. All of this may help an analyst in breaking a MAC. Putting 128 new bits from a secure PRNG limits helps to alleviate this possibility.

But you still have to watch your passphrase. And if you are going to put a PRNG into the implementation, it is better to get k and k' in a different manner. If R() is the PRNG and H() is a hash function then we construct k and k' by seeding R() with H(user_passphrase) and grab 16 bit (or 256, or whatever you like) blocks from R() for use as k and k'. The prior method of getting k and k' seems secure, but for the few K of RAM needed for a nice PRNG, it seems silly not to use it.

Implementing programs to do this sort of deniable encryption is a rather trivial matter. Source code to strong hash algorithms and good streams ciphers is widely available, and simple to use.

It is tempting to just implement the basic winnowing tools and let the crypto be done with an external program. I advise against this as it requires more keys to be remembered, and when under actual pressure from law enforcement to reveal a key you may not be able to get your wits together and give the right key. Accidents happen - you don't want to give the wrong key. It is also preferable to add documents of a "sensitive" nature for the express purpose of giving up to law enforcement. Maybe encrypt a few articles from Phrack and a few porn pictures. Such material seems more likely to get encrypted than Hamlet, and will give you a better alibi regarding why you have that ciphertext, not that you should ever need one, but such is the state that we live in. Be prepared.

Shouts go to Szyth and Wipeout for good hacks, lots of beer, and really sick looking code while under the influence.

References and related material:

[RIV98] Chaffing and Winnowing: Confidentiality without Encryption, Ronald L. Rivest, http://theory.lcs.mit.edu/~rivest/chaffing.txt

[CAN97] Deniable Encryption, Ran Canetti, Cynthia Dwork, Moni Naor, Rafail Ostrovsky, ftp://theory.lcs.mit.edu/pub/tcryptol/96-02r.ps

THE BACKYARD PHREAKER

by D-Rez

For those of you who live in the suburbs or small towns, did you ever wonder, "Hmm, there must be more controlling my phone than the 5"x10"x3" box on the outside of my house"? Well, right you are. However, the box controlling your (and all the other people in your hood's) phones is not behind locked doors. It is usually on an accessible shaft, not more than a few feet from the curb. Look for the big telco box, it usually has the telco name on it and sticks up a good four feet from the ground. This is the neighborhood telco box.

Now, one would think, "This box which controls all telecommunication in the area must be under lock and key, right?" Wrong. Your local telco thinks your lines should have no more protection than an odd shaped hole. This can be undone with a special wrench, or with needle-nose pliers. Unless you happen to look a lot like a telco serviceman, breaking into one of these boxes might look a little suspicious, so don't be a damn fool. So much of hacking/phreaking is just common sense. A modicum of discreetness can save you hours of dealing with local police officers.

Once the box is open (it was already unlocked I just opened it out of curiosity, officer) you will feel right at home. The same kind of setup you have at home (black wirebed wire, sometimes a jack) is present here. Forty-fold. These are all your neighbors' phone connections. Unplug one of those jacks, poof there goes Joe Blow's line. Connect your handset to a pair of terminals, and you have access to this phone line. Child's play.

This system is easy to phreak, but easier to destroy. Should one be so motivated, one could, say, rip out all the wires and run. This would cause havoc among your neighbors, and certainly make you far less popular with the locals. So, for the sake of people who didn't do anything to you, please don't go randomly ruining service for a whole district because you can.

However, people tend to get a little nervous when their phones suddenly go dead. And, if you are caught, the redial on your handset can be used against you. So, for the backyard/suburban phreaker, here is a list of handy tools you can use as a "safety net," to ensure Officer Friendly doesn't suddenly come around the corner.

1. *Line in use light* - They sell these at Radio Shack for $12.00. This is a little box with a light on it - when the light is on, the line is in use. Before utilizing a random line, check yourself with this pocket-sized insurance device. Makes a great gift. (Humor)

2. *Tone dialer without redial or memory* - Should you be caught after the fact, won't you feel like a dumbshit if the last number called on the line you phreaked is the number that pops up when "redial" is pressed on your phone? A tone dialer prevents all this. Since the phone only remembers the numbers pressed on the phone keypad, you'll be smart to do all your dialing with a tone dialer, sans redial or memory settings. Although laws are so vague that you can now practically be arrested for having a phone and alligator clips, it's better for you if they can't prove anything. Dial with a tone dialer, you play it safe. Dial direct - too bad so sad, you're on your own.

3. *Common sense* - OK, for all you non-geniuses, first and foremost - *Don't dial lines connected to you in any way!* That means don't dial your house, your cell phone, your pager, your girlfriend, your favorite BBS, your mom, your boss, or any numbers dialed a lot by your home phone. You've been warned, they do keep records. Secondly, clean up after yourself. Wearing latex gloves would be a good idea, but not leaving business cards also helps out. In conclusion, you weren't there, and you should do everything in your power to make it seem that way. That means closing the box after you're done. "Holy shit, where are my car keys?" is simply not acceptable.

Keep your head about you, don't do anything stupid, and watch your back, and you can have hours of fone-phun in your gated community. Act like a moron and get your ass thrown in the meat clink. Happy phreaking. Don't tell anyone I told you so.

I do not, in any way, encourage criminal behavior, nor do I promote destruction of telephone company property. I also do not condone or encourage the activities listed above, nor have I or anyone I know ever performed the acts mentioned above. Please. Don't fuck with people.

expanding caller id storage

by Datum Fluvius

The telephone company sent you this tiny little 25-call memory Caller-ID box for free in the mail when you signed up for Caller ID. You want a better box with more memory, but the $59.95 your phone company wants for a 99-call box just might be better spent on something else. Like the extra charges for having caller ID! *Hmmm.* What to do?

Easy... just hack it!

The two units I'm reviewing are both called CIDCO model PA. These units use the same software, CA1 version 4.1, which they proudly display when they first wake up. The difference is in the hardware. You can find the PC board revision letter on the sticker inside the battery compartment, at the extreme lower left corner of the sticker like this: "J4.1". Don't worry if yours is different than mine. Just read the procedure and I think you will catch on to CIDCO's method of selecting the memory capacity for a given unit.

Assembly 553, Revision "E"
Assembled 1997

The memory capacity jumpers are on the battery side of the PC board on the left side. You don't have to unscrew the PC board from the faceplate and LCD screen. Yay! When jumper "C" is closed, the capacity is 25 calls. Open the solder jumper with a sharp exacto knife or soldering iron and the device should wake up and display "99 calls, CA1 Version 4.1." This jumper is especially easy to spot because the poor factory slave who soldered the thing dabbed the nearby pads ("D" and "B") with red epoxy to avoid any spillover. Her job was later designed out of the process, however. (She's picking up cans in your alley as you read this.)

Assembly 553, Revision "J"
Assembled 1998

The memory capacity jumper is a single pair of pads, marked "C", and is very hard to spot. First, you will have to unscrew the PC board from the faceplate in order to look for the jumper (4 screws, one in between the jacks). The jumper is just to the right of the big black blob of chip epoxy, above the C 12 capacitor. It looks like an unused capacitor pad. A very careful and sharp exacto knife is more useful here than a cheap soldering iron!

Just like the rev. "E" this jumper is closed when set to 25 call capacity. Open it up, and you have 99. The other capacity (and most program/test) options are missing. Apparently not many folks bought the mid-range units....

That reminds me - what the hell are those program/test pads for? What could we find out by using them? They are present on the revision "E," so it might be hard to go out and order a test unit now, but any older unit should work....

The Revision "E" pads are labeled, in order from top left:

K3	(???)
EN	(enable?)
-TST	(test?)
-LD	(load?)
D	(Capacity jumper)
C	(Capacity jumper for 25 calls)
B	(Capacity jumper)
A	(Capacity jumper)
RS	(reset?)

There are some similar pads on the revision "J" but they are labeled:

JMT	(jumper, open)
-LD	(load?)
C	(Capacity jumper for 25 calls)

I have not tried out anything on these. Anyone for some exploration?

CLLI CODES EXPLAINED

by Crossbar

Common Language was developed for use by all Bell Client Companies (BCC). This Common Language is used in prepared Work Order Record and Details (WORD) documents. Common Language is presently being used to prepare records of circuits, trunks, and equipment for the Trunks Integrated Records Keeping System (TIRKS). In this documentation I will be explaining the construction of Common Language Location Identification (CLLI) Codes.

The CLLI Codes are used to identify particular telephone buildings within a given geographic area. They specify a particular work force or administrative group within the building. The CLLI codes are also used to identify the non-building locations. These codes are made up of 11 alphanumerics that identify the telephone building. They are made up as follows:

Place (XXXX) (character position 1-4)
State (XX) (character position 5-6)
Building (XX or NN) (character position 7-8)
Entity (XXX) (character position 9-11)
(Switching or Non Switching)
Non Building Location (ZNNNN) (character position 7-11)
Customer Location (NXXNN) (character position 7-11)
X = Alpha, N = Numeric

Place Code

The Place Code is considered to be a municipal locality such as a town, city, or community. Military locations, local names, or major shopping centers might also be referred to as a Place Code. The Place Code is a 4 character alpha-mnemonic. An example of one would be DNVR for Denver, Colorado.

State Code

The State Code is a two character code representing a particular state. Provision is made for entering a Province of Canada Code or a Country Code if applicable. An example of one of these would be CO for Colorado.

Building Code

The Building Code identifies the particular building within the geographic area. The building may be represented by a two character alpha code, or two digit numeric code. An example would be XO or 56. That example means nothing to me. If it is a building, like a CO in Ohio or such, then it is by chance, I swear. If the first letter in the code happens to be an X, such as X1, then it means that the building is an Independent Telco Location.

Entity Code

An Entity Code specifies any unit or equipment, work group, person or job function which is directly related to message and/or data switching and termination. Entities are assigned to two broad categories, switching and non switching. They are made up of alpha and/or numeric characters. An example of this would be 7S4.

When it isn't necessary to specify a particular group within a building, the Entity Code may be dropped and a CLLI consisting of a Non Building Location will indicate a site or position of telephone equipment other than a building. The Non Building Code is a 5 character mnemonic code. These are the abbreviations for position Seven.

B = International Boundary Crossing Point
E = End Point
J = Junctions
M = Manholes
P = Poles
Q = Radio Locations
S = Toll Stations
X = Independent Company Non Building Location
N = Customer Locations
U = Miscellaneous Non Building Locations

STETEO is Satellite-Earth Orbit. This replaces position 1 through 6. The Radio Code completes the code.

Customer Location

A Customer Location may be a military installation, a customer located switched service network, a customer located Centrex installation, or a location required for Trunk forecasting and design work.

I hope this will help you in your quest for knowledge. Remember, all knowledge is useful.

HACKING RESNET

by jk

The RESNET (RESidence hall NETwork) isn't a single entity, it is a cookie-cutter approach to networking dorm rooms at universities. The people responsible at each campus basically get together on a self-help listserv, tell success and horror stories, and sort of come up with a plan for what they want to do and how they want to do it. It is an environment that is full of possibilities for exploration.

To learn why it is so disorganized, you have to understand the politics. RESNET isn't a unified network at all and there are a lot of egos and posturing involved. Universities tend to do their own thing and have a hard time holding onto good people (who can leave and get a lot more money elsewhere in industry once they get good). In addition, the people who pay for the equipment (housing) are usually a separate entity from the university itself, both in mentality (real-estate) and financing. The financing issue creates most of the disorganization, along with the initial power-plays involved when RESNET first gets installed.

If the (experienced) network people had their way, things would be locked down pretty tight. That costs money, but it is the housing group's money. This is usually the first power struggle since the housing people want something that is cheap and inexpensive and the networking people want something that is secure and (more) expensive. After much infighting, this basically boils down to having a network infrastructure that can be made secure, but currently isn't. If you're in a RESNET that wasn't recently established, chances are excellent that cost would have prohibited some of the more secure solutions (switched vs. shared network ports, for example).

The RESNET goal is to make the user use DHCP to configure their IP and force them to register themselves on a web page. When someone sends off fan-mail to the president, the people responsible want to be able to say that they've made a best effort to be able to hold that RESNET subscriber accountable (someone's head on a platter). One important aspect is that they want to totally automate it as much as possible so they don't have to have that much manpower to provide reasonable service. Basically, they want to be able to hunt you down if they find you doing something you shouldn't, they don't want you to set up a local server, and they don't want to give you any reasonable expectation of a service they may want to take away later (even if they can't really enforce it at that point in time).

Using DHCP has a number of good points for them. It is slightly biased against non-desktop operating systems (if they have to help you, they want you to have something they understand and good *NIX hackers are scarce), it randomly assigns you an IP address and can be configured to assign you a new one at sometimes unpredictable intervals, and you get a generic unpersonalized hostname. They can do very little (DHCP does most of that by default) and pretend they're offering a service of convenience. They don't want someone setting up another Yahoo! in their dorm room. If they could think of a good reason, they would probably write up an AUP that would find some way to say that you can't have incoming connections. Most of them aren't too worried about it but they should probably be with server apps appearing for win98 and macs. They don't want to spend the money to enforce it, which would mean a high-performance NAT device between the dorms and the backbone with a random-few:many IP setup.

DHCP also provides the side-effect that they get your ethernet address from your NIC (which is supposed to be a unique number) tied to an IP address for a time interval, and when you register it gets tied to the "resident." They only want one device/person, both for security (typically unused) and cost (they want you to buy their service; if someone sets up a hub in their room and networks the general area, they don't get the money). They would also like to make people responsible for their port, so what comes through their port is their fault.

The usual setup is to have a slightly modified DHCP server that will serve crippled and non-crippled IP addresses. If you're registered, you end up with a static entry that points to working DNS servers, routers, whatever. The dynamic addresses that get served to unregistered NICs point to the registration server. The trick is to get it so your average person will boot up, bring up their web browser, and find themselves aimed at their registration server if they haven't signed up. That is often accomplished by sabotaging apache, setting up a fake root DNS server, and adding a few virtual hosts on a *NIX box so that any remote HTTP page gets directed to the server, where apache drops you into the registration page for anything it isn't serving.

Know thy enemy! Many of the RESNET sites are using a slightly modified version of one package. Visit http://www.rit.edu/~rarcsys/dhcp and look.

Problem (for them) #1: You don't have to use DHCP. Other than by written policy and obscurity, they can't crawl onto your desktop and force you to use DHCP. You can statically configure your box to whatever works, usually by shoulder-surfing one of your friends when they have their TCP/IP control panel open. Most of the RESNET solutions are running on something cheap like Linux and using the ISC DHCP daemon. One of the newer features that later versions have is to check and see if an IP address it is about to assign is in use. If it is, it marks it "abandoned" until 2038/01/19 (at least for dhcp-2.0b1pl1). Chances are that if you grab someone's address, the server will work around you, quietly assign the victim a new address and leave you alone for 40 years. You ought to be graduated by then. The administrator has a list of addresses to hunt down, but it is probably a low priority if you're not being a squeaky wheel.

If the network folks had their way, you'd be connected to a VLAN-ready hub that can assign addresses dynamically that had lock-out security features. Plug in with the wrong NIC or more than one NIC, you get dropped and your port locked down (perhaps requiring human intervention to fix). Based on what NIC you use, you get put into a crippled VLAN or a working VLAN (depending on if you're registered). This is a much more secure scenario but it requires some additional help for the network folks. In particular, they have to interface with whatever protocol the switch is using to assign a particular NIC to a particular VLAN (if their switch can do it at all - another equipment cost issue). Those are often proprietary protocols, with the vendor wanting to sell you their security solution. The housing folks tend to nix that extra expense since nobody has proven that their little resident cuties are criminals yet. If nobody has abused it, chances are that they won't have this type of security in place yet.

Problem (for them) #2: If you're using *NIX on a PC, can get a valid IP address once with DHCP, hard-code it and set up NAT, you can hook up a bunch of machines behind yours with nobody being the wiser. They may try to change it from time to time, but with the way the DHCP spec is written you are perfectly well within your (DHCP protocol) rights to try to use the same IP address all the way up until your DHCP lease expires. I don't know what the ISC DHCP client does on a *NIX box if it has to change the IP address mid-session, but you can probably live up to the letter of almost all their rules without any problems.

When you have a working connection (registered or not), it is time to see what you can see. The networking guys aren't giving you switched ports for performance, they're giving them to you for anti-eavesdropping security. A switched port will pretty much stop you from seeing anything that isn't a broadcast or multicast, and almost nothing of interest is contained in them, although they may reveal interesting bits of information (IP addresses on that segment via ARP, other machines via IPX SAP, etc.). Those switched ports cost money and some people won't pay for that. They used to cost a lot of money, so older installations are probably lacking. If you're not on a switched port, grab your favorite packet sniffer and see what there is to see. Your average fellow student probably isn't using SSH.

If you're on a shared hub, you should be able to see all the local traffic from your neighbors. If it doesn't have a bridged uplink port (unlikely), then you might be able to see the RESNET backbone traffic as well (all your neighbors). Any site that doesn't offer switched ports is at risk for all kinds of sniffing/insertion attacks.

One of the benefits of RESNET is that you're typically on the campus and can have high speed

access to the backbone. This is traditionally something that the network folks aren't really keen on. Right now, their main worry is off-site hackers since they tend to have the local machines locked down. Off-site links are a lot easier to deal with since you can drop a filter on a T1 with no real speed hit. 10MB and above can cause a serious loss of throughput, although some newer flow-based algorithms can reduce that a lot. With RESNET, they now have a bunch of unknown kids with root access to their own, local machine on a LAN who know all about their security by obscurity. That is usually a pretty big mental shift for them and they don't want to consider (budget!) costly consequences until someone holds a gun to their head. If the RESNET hacker doesn't become the squeaky wheel then they can get away with a lot.

Unlike slow WAN situations, high-speed LAN access can cause some problems for security. Any firewall or other bottleneck is going to stick out like a sore thumb when you have 500+ switched-10 connections trying to go through it. If you get a high-performance firewall or a lot of low-performance firewalls working in tandem, you're going to add cost which the housing folks aren't going to like. The network folks will have wanted to keep their options open, but they're probably not going to have a filter in place when people start hyping about all the cool things they're doing for the students. Bandwidth, much like disk space, tends to get filled to capacity very quickly. If they don't put a firewall in place quickly, people aren't going to want it for the added expense or the bottleneck.

You may think these non-decisions are obvious, but paper-pushers are a different breed, especially when their money is involved. They seem perfectly happy to be reactive and fix a problem after they get hit. Up-front cost is everything, and long-term savings don't mean a whole lot when you're living year-to-year on a budget. The obvious analogy of standing on the train track and getting off before or after the train goes by is totally lost on them.

What tools do they have to track you down? Potentially lots. It really depends on the hardware they're using, their competence, and the tools they have available to them. The easiest bit of information they'll have is your IP address, since anyone who noticed will log that these days. If it is on the other side of a router, your MAC will be unavailable. If you registered with DHCP, they'll quickly track you down and turn off your port. They may be able to blacklist your NIC so you can't use it in any port. That would be inconvenient.

Depending on their router setup, they'll typically know what network segment you're on (host routes and source routes don't work too well in the modern LAN, but you never know). In your average RESNET, these tend to start out big (a building) and narrow down as required. If you haven't left a permanent record (registered) or they're not strict about what MACs are used on any given port, they pretty much have to catch you real-time by looking at ARP entries on the nearest router and bridging tables on the switches (to find out what port a MAC address is behind).

One of the security options some switches have is the ability to lock a port to one MAC address. If you're hacking with a fixed MAC on a locked port, the hunt is going to be pretty short. In your favor are convenience (public access areas, that they can't lock to one MAC) and laziness (if they have to unlock a port every time it locks, some human is going to be bored out of their mind). A few late night calls saying your port got locked for no good reason might convince an RA that it is more trouble than it is worth.

Routers are a small problem since they are passive learners and will hold onto ARP addresses long after they're out of use (10+ minutes). Switches are a little easier since they tend to clear their MAC tables when the port loses link. Do the dirty deed and drop the link. They're going to have a hard time finding out what port the MAC was behind.

Some SNMP-ready switches can send a "TRAP" to an SNMP management station when a port comes up and down. This is usually disabled by default since it generates a lot of traffic and notifications managers normally don't care about. Some of the clever RESNET sites look for the link up TRAP and then start probing for MAC addresses periodically on that port. This is a pretty good proactive way of doing it. The ways they might probe are pretty custom since it usually requires someone fairly competent to set it up, so a little inside knowledge will work wonders. If they only probe once at some interval after the link comes up, you only have to wait it out and then send your traffic. If they probe periodically, you have to use your unregistered MAC in between probes and drop the link before the next probe (clearing the MAC table entries for your port).

If you can find someone foolish enough to leave some IP-relaying software turned on, by all means bounce it off their PC and use their MAC. The average fool won't be able to track you down and probably won't notice until someone tracks him down.

Switches make it very hard for network administrators to sniff your traffic even if they wanted to. Beware that some switches do have the capability to echo everything on one port out another where a sniffer can be attached. If you can take over a switch, you could use that to your advantage. Beware that some switches also have authentication traps and some keep track of various failed attempts, so someone might notice and wonder what is going on.

If the network folks get their wish and you're doing MAC-based VLANs, you're probably fooled. A good one will puke the port when it sees a foreign MAC trying to pass traffic. They're also a lot more likely to log and timestamp MAC-to-port associations, leaving an unwanted trail of breadcrumbs to your door.

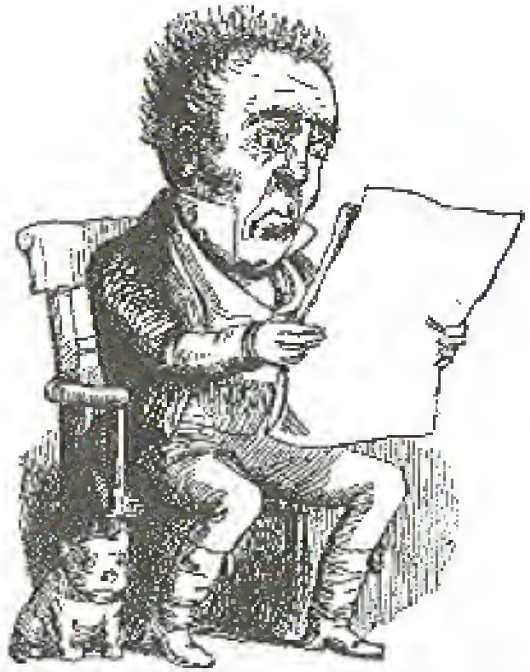
If you're not on a switch, things are going to be much harder on anybody trying to track you down, although they have different options. The bridge tables only say which side of the bridge the MAC is on. Usually you have repeated ports in multiples of 12 (often 24, depending on the age of the hardware) and a given MAC might be behind any one of them. They'd have to go door to door or eliminate everyone else *and* catch you in the act. If they stick their own sniffer out there, they'll be able to see everyone's traffic. Depending on your network folks, that may or may not be permitted. Many of them have some kind of privacy policy, although they can pull all the stops out if you're being a serious pain in the butt.

If you end up behind a layer-4 switch, you have all kinds of possibilities. Layer-4 switches are usually made by vendors that wanted to get into the routing hype (and markup) but couldn't make it work. They usually only work for IP, but they make router-like decisions based on what IP address you're using. Where they usually fail is with broadcasts and the doors they're supposed to be in. You can get a lot of information leaking from network to network that you wouldn't get in a properly routed environment. DHCP causes many vendors to have fits, so it is debatable if you will find them in a RESNET environment.

One last thing to consider is using multiple MACs and/or IPs on the same machine. One of the reasons the RESNET folks want to restrict you to DHCP and a registered MAC is to make it easy to make draconian decisions (and use MAC-based VLANs and other MAC-based security at some point in the future). One of the reasons they'd like you to use Windows or MACs is to make you use an operating system that doesn't make it too convenient to break what they consider "natural laws" (but are instead mostly average and typical behavior). If they lock out a MAC without tracking you down, they're counting on you having to spend $50 to get a new one as a significant deterrent. If you make one up (or use someone else's), that deterrent goes out the window. Most switches aren't aware of the higher layers and will lock on MACs but not IPs. Doing virtual IP addresses on a *NIX box so you have multiple IPs attached to a single MAC might exploit some fundamental flaws in their thinking and planning.

Most NICs can handle several different MAC addresses easily without bothering the CPU (mostly for multicast support). Given the right device driver, you might be able to add a randomly generated MAC to your card (so it will recognize it as itself and process its traffic) and bind your "special" applications to it. Anybody looking at your setup will see nothing unusual (no extra hubs, etc.). They'd probably have to track you down real-time and catch you in the act.

It would tweak the most minds if you use a firewall-type setup for your abducted address and only allow traffic on the ports that you are using. If someone is trying to track you down, they may try to ping you (ICMP) or use some other well-known ports. This may be the first thing they do if they're trying to decide if they can catch you red-handed online, rather than trying to pick up stale breadcrumbs. If they telnet to your assumed IP address and it tells them your PC's name in a banner line you're not going to feel too clever. If it totally filters and ignores traffic you're not expecting, it should make it nearly impossible for them to make you reveal yourself beyond your MAC entry(s) in the bridge table.



LETTERS

Warning

Dear 2600:

Attention fellow phreaks and hackers. Four of my friends have gotten arrested in a period of 1.5 months, each at a separate event. It turns out, as they were shoulder surfing, they were doing it to undercover cops, hotel clerks, or they were being tailed by cops. ATM's as well as calling cards. Most cards are marked (the ones they give decoys). It happens mostly near large banks of pay phones near banks, buildings, and malls. Beware! Especially in the Manhattan area. These cops are also using scanners a lot of the time. So keep your eyes open."

Lucy aka Boudewiser

Perhaps you should keep your brain open to an intelligent thought or two. One of those might be the realization that the kind of thing you're involved in are not plain and simple fraud and have nothing at all to do with hacking. We're not interested in your little crime ring.

Store Section

Dear 2600:

On page 5 of your 15:1 issue it reads, and I quote: "We back Gem (Barnes & Noble) completely in their rights against neighborhood censors who try to shut them down because they don't like the pictures in a book..." Surely you are, I hope, referring to the recent child pornography protests of Barnes & Noble. Just as you would prefer not to be used, abused, misunderstood, and exploited as "Generation X punks," I doubt these children pictured would consent (if they were old enough to protest) being touched and fondled in front of a camera for the amusement of a few sick individuals. You and your magazine stand for freedom of rights so I hope you are recognizing the rights of an underdeveloped, helpless child to live an emotionally healthy life.

Bluebell

It's funny how people hop into whatever they're told without checking the facts first. We strongly doubt that Barnes & Noble would ever sell child pornography. The controversy comes as a result of a campaign by conservative groups (those on the Family and the American Family Association) and it's targeted against two books, Age of Innocence by David Hamilton and Realized Innocence by Jock Sturges which depict young, not obscenity. Of course, states like Alabama and Tennessee fail to make a distinction between the two and by leading a communist, manipulative campaign people think what they say is true. Go find the books and make your own conclusions.

Dear 2600:

After reading the articles that were written about Best Buy in 15:1, I've decided to give a little of my own amateur input about Office Max.

Like Best Buy, the climate controls for the store are located out of the store and sent to each store's computers and then the in-store computer will change everything accordingly.

Passwords for Office Max in store computers typically follow the same pattern.

Login: store

Password: 9mm, ammo, or ammunition where nnn is the store number found on any business card or receipt.

Just about anything can be changed by those terminals located throughout the store. Prices, label descriptions, how many labels to print, stock, UPC's, etc. However, the same computers are rejected from backup every Saturday.

The telephones at Office Max are almost always the same. 59 gives you the intercom. 2-digit extensions are usually located on a key under the phone that slides out. Almost all the telephone jacks at Office Max are labeled. This includes the lines used to verify credit cards and the stock data line used for getting climate instructions.

NS

Dear 2600:

I'm not nor have ever been a hacker/phreak but I have had experience with Energy Management Systems (EMS). Mbius was not entirely correct with his piece "Even Better Still," regarding the EMS at Best Buy, which would apply to most of the larger stores that use them.

These systems are used primarily to reduce costs of utilities and secondarily for convenience and effort within the stores.

The EMS is a Programmable Computer, or PC, and is totally self-directing, except for various local sensing devices used to modulate lighting and HVAC units. They have battery back-ups in case of power failures and are usually programmed for a year or more in advance adjusting for daylight savings, store hours, outside temperatures, seasonal darkness outside, et al.

The units are not controlled from a remote computer but are programmed remotely, or adjusted for some special occasion. Local management can also open the door to the EMS PC and operate override switches when necessary, and hopefully they know what they are doing. The usual programming and maintenance is done by qualified technicians or engineers, or occasionally by some semi-bozo who wants to impress his ego.

It wouldn't create a disaster if he did attempt to fuck it up because as soon as someone in the store realized something was wrong, they would call the service people who would reprogram the PC to its original parameters via a phone connection. Their home computer has every customer's EMS PC specifications in its file for instant use.

Frankly, I think that if Mbius had a brain he would play with it instead of his pokemom.

SOUPN

Dear 2600:

This is regarding Greyhawk's letter on Babbage's employee software checkout policy (15:2). I worked for Babbage's and they do let employees check out any software in the store. They then reseal it when you bring it back. They also let you check out all gaming consoles and games (i.e., Playstation, etc.). They claim there is nothing illegal about it, as long as you delete it. Basically Babbage's employment = minimum wage + free software.

Bad Inc

Dear 2600:

In response to Greyhawk's letter in your last issue, yes, it is true that Babbage's (software, etc.) employees are authorized to check out (basically anything in the store, as long as it is returned within 48 hours and in a sellable condition. As I am a Babbage's employee, I can tell you that it is also true that these stores do repackage items that are checked out or returned as defective. Although this does occasionally pose a problem (when the product uses a unique cd-key, mostly games like Ultima Online and StarCraft), but these products are usually returned and sent back to corporate, who ends up absorbing the cost.

In terms of buying, the employees who copy this software are at fault as the check-out terms (at least in my store) state that the software may not be copied, and doing so is grounds for termination. To tell the truth, most software shipped to us is sent in such a poor condition that we need to shrink-wrap it anyway, and most people are so anal about things that aren't wrapped. To whatever manager said "you can't copy CD's anyway," that's bullshit and most people who work at Babbage's work there for the "benefits." I know my manager does.

Op. Code

Dear 2600:

It has been company policy for as long as I can remember. I started work at a Software Etc. in '94 in Fargo, North Dakota and worked there up until the store closed in '96. Company policy for the time Babbages and Software Etc. were owned by our good friends at Barnes & Noble) allowed employees to take software home for a week and "get to know it" so we could do a better job of selling the product. Policy stated that we weren't allowed to copy disks or leave the software installed on our computers after they were brought back. At that time we would take the product to the back room and shrink wrap the box to look just like new. We weren't supposed to check out 3.5 inch disks because some software would write the user's name to the disk. But on more than one occasion my district manager told me to just make a copy of the first disk.

Software Etc. seemed to get the politics off of keeping track of customers who bought software back at an irregular rate. They believed these people were taking advantage of the return policy that was in place at the time, copying the software and then bringing the product back for a full refund. What they really needed to do was watch the employees. They even copied software during their shifts on the in-store demo computers!

Cas

Dear 2600:

Just writing to let y'all know about the letter from Greyhare in issue 15:2. Yes, this is true. I used to know someone who worked for Electronics Boutique, who used to do the same thing. Employees were allowed to take games home to "test." That way they could tell potential customers how the game was. Of course, you were supposed to delete the game when you were done... Incidentally, I'd be far more worried about getting a virus than being "shrunked on by store employees."

Pirated!

Dear 2600:

I just read the letter from your 15:2 issue from Greyhare about Software Etc. employees being able to take home games and bring them back to sell at full price. I would just like to confirm. I was best friends with a Software Etc. manager for a while. He could take any game home for two week periods, providing that they had enough copies left at the store for the customers. When he returned them, they would shrink-wrap the plastic back around the box and sell it as "new." Software Etc. and Electronics Boutique still have a "7 day no questions asked" return policy anyway, so there is no need to become an employee to take advantage of the "freeware" program. As far as I know that's nationwide.

entropic

Well, it didn't take long for our readers to confirm this practice, which seems to be widely known in the software industry. Just further proof of the hypocrisy the software police call reality.

Dear 2600:

Thank you for publishing the letter to the editor called "Bookstore Monopolies" (15:1), where rj eleven recommends the website www.booksellersunion.org. There is a Barnes & Noble employee working at my local college bookstore who has legally posted information in his break room regarding employees' rights which has been continuously ripped down by his managers. Including letters to the editor like this in your magazine provides important moral support to those poor workers who have to live with injustice everyday. Thank you so much for your help.

GW

Dear 2600:

I really don't understand the fascination with our (Barnes & Noble) databases, but I can tell you, you're in for a long, dull time messing around with them. Believe me, as an insider, I know...

One thing you guys should know: there was no corporate-wide memo regarding you guys at any level. I'm in a such a position that, were there one, I'd know. I think you spoke to a couple of apathetic-looking-for-a-thrill part-timers when you verified this phantom memo. Perhaps more informed and truthful sources would be better utilized in the future.

My fellow booksellers and I await the latest 2600 expectantly, and we would never just strip the copies for petty revenge. We get a kick out of the fascination with us, and the amount of "crap" you're fed (and believe) from "employees." That whole "33 salmon" password? A dud. All the "x1, x2" stuff? Available on any receipt when you purchase a zine, paper, coffee, or food. And as far as getting into credit card numbers, going through the garbage would be faster and easier. (By the way, we don't use the same passwords or codes on all the keypad doors, either. But, if you want a look at our break room or janitorial closet, ask for me, I'll show you. It's no big deal.

Thanks for all the fun! And, by the way: doesn't Borders use computers, too?

Allegra

Talk about steering us to the competitor.

Help Needed

Dear 2600:

I was wondering if you could send me the bibliography for the article "A Brief History of Postal Hacking" from 15:1. I am very interested in researching this field more. Thanks.

JD
West Columbia, SC

Just go to your local post office and ask for more information. If they say they don't know what you're talking about, it means come back in one hour when the supervisor isn't around and ask again. You may have to ask a few times before you advance to the next level.

Identity Problems

Dear 2600:

I am a newbie hacker. I am 14. I am also female. On IRC, in the hacking channels, I constantly get picked on. They call me the "Female Lamer!" I have done nothing to them to make them think this. I don't sit there and brag about myself and my hacks like they do. They are just sexist pieces of shit who think they rule the world of computers. They pick on me because I ask questions. And because I am female. May I ask, what is so bad about a question? In school, they tell you to ask questions, then you get shunned for it and called a lamer on the net? This is not fair. Is there anything I can do to make them see that because I'm younger, less informed, and *female* they have no right to pick on me?

SnoWeenie

Since you made no less than four references to your gender, we suggest that you make this less a part of your identity since it obviously is causing you problems. On the net, it's not essential information anyway. You can be whoever you want and start over as many times as you need to until you find something that works out.

Mitnick Feedback

Dear 2600:

About Kevin Mitnick being cut off from technology, it just isn't right. I mean, what can someone do with a laptop and no modem? Nothing! He should be free to review the evidence when he wants to. They must have something they don't want leaked to the public or they would a) let him look at the evidence, b) give him a trial, or c) give him bail. Keeping someone for so long without a trial is inhumane and a violation of his constitutional rights! Just wanted to be heard.

Philight

Dear 2600:

I have put my "Free Kevin" sticker to good use. 50,000 cars a day will see it while they wait at this red light/overpass. How about a "Best Placement of 'Free Kevin' Stickers" contest?

Wheetablx

Good idea. Send us photos.

Dear 2600:

The comment you put inside the front cover from Mike Godwin (14:1) versus the comment in the cover of 15:1 just shows how even people who don't like hackers realize how fucked up the government's case against Mitnick is.

Columbus, OH

We've found this to be true just about everywhere we've spread the word to the public.

Dear 2600:

First off, allow me to extend my compliments as always on an excellent, informative magazine. I have read it religiously for several years now and have both been amazed at the wealth of information I discovered and appalled at the outrages that go on right under our noses. The Kevin Mitnick outrage is the reason I'm writing this letter. Enclosed you will find my check for $100 for the Kevin Mitnick Legal Defense Fund. Kevin's plight has been the most astonishing travesty of "justice" I've ever heard of and I'd like to step in and do my part to draw the line in sand. If we all sit back and do nothing when things like this happen, we are just giving the government our permission to rob us of more of our freedoms a little at a time.

You may also be pleased to hear that my wife, a college instructor, is now a regular reader of your magazine also. In fact, she insisted that I contribute more money than I had originally planned to! Every quarter your magazine would come in and I would devour it muttering about the injustices that were happening to people like Kevin Mitnick and Bernie S., and eventually she asked me just what the deal was. I let her read Kevin's saga and she was simply stunned that such a thing could be allowed to happen in America. From that day on, she was a vehement reader. We are both doing our part to educate everyone who will listen about Kevin, Bernie S., and 2600 in general.

MW
Solon, OH

Thanks from us and from Kevin.

Dear 2600:

I have been reading and enjoying 2600 for a number of years and I have to say you're starting to sound an awful lot like the governments you're so afraid of. I keep hearing a lot of "poor us, that bad 'ol media just unfairly pickin' on us poor innocent hackers. Don't they know we's the good guys?" Give me a break! I've been hacking since before there was a distinction between hackers and crackers, and yes the stupid media, with the help of the stupid crackers, have lost the distinction between the two.

But not even you can deny that hackers (meant in the media sense) pose a serious and dangerous risk to business, government, and yes individuals. Your magazine is becoming more a political agenda than a "free speech, free flow of information magazine." While we're touching on this (the political aspects of the mag), the information you're spewing about "poor innocent" Kevin Mitnick is just as distorted as anyone else's. I notice you seem to almost always overlook the fact that he had all that credit card information, oh, I know, he's a good guy, he'll never use it for evil purposes. Unfairly imprisoned, no trial, um, can you say *pleaded guilty*, boys and girls? Or is that not being mentioned for a reason?

The fact of the matter is, Kevin sucked as a hacker. He got lucky and he was stupid and he got caught (that's how the game is played, if you don't like the rules, don't play). The good hackers are the ones you never hear about.

Finally, do we really care what the media or general public thinks? Your attempts to "educate" people about the righteous cause of the hacking community is going to be real successful as long as there are Kevin Mitnicks out there. Do you not see where people might get confused when on one page your new "reg" mag is saying, don't fear us, embrace us, we're the good guys, etc. And on the next page you're saying "How to Hack your ISP" and "Tips On Generating Fake ID" both clearly the reading choice of your average law abiding citizen.

This magazine, our magazine, is supposed to be about the free, open, and honest exchange of information and ideas, not a political soapbox. Let's get back to what you do best and inform, educate, and entertain your readers. If we wanted sermons on the good works of Kevin Mitnick, we'd go to church.

Mafker
(I suspect you've never heard of me)

No, we never heard of you so that must mean you're one of the "good hackers." And we're not even going to get into the whole "cracker" fiasco this time around. Let's start by going over the things you missed while in a coma or ordering Napalm or whatever caused these wide gaps in logic. We've mentioned the credit card file repeatedly. It was used to vilify Kevin in a most unfair way. The file itself had been floating around the net for

ages yet Nature had refused to even acknowledge this fact. We reported on its existence a full six months before a copy was found in Kevin's dwelling. It was easy to get. Hundreds, perhaps thousands, of people wound up with copies. We don't know anybody who wouldn't want to see if such a thing really existed. That is why Kevin had a copy and further proof of this is the fact that not one of these numbers was ever used by him. Even though it would have been an easy way to get free stuff, Kevin is not a thief. But by maintaining that as the first paragraph of his story we, for instance, the New York Times, made him look like a common criminal.

As for pleading guilty, you've got your facts confused. Kevin pleaded guilty in North Carolina to possession of cellular MIMs that were used to make unauthorized phone calls. (This allowed him to be extradited to his home state of California and he long ago finished serving that sentence.) You may consider this to be the same as stealing something tangible but all that accomplishes is to make the real theft more excusable. This was literally the only way Kevin could communicate with us, as he thought with half the FBI chasing him around the country. Taking out phone service in his own name may have satisfied your moral standards but it wouldn't have done very much for Kevin's freedom. So the question remains, why was Kevin running in the first place? For associating with a known felon who later turned out not to be a felon at all? For not reporting to his parole officer when phone records have proven the opposite? It doesn't take much investigation to see that Kevin was targeted - why, we can only speculate - and that all of the missing charges against him are for absurdities like copying worthless files and making a few free phone calls. For this he deserves more prison time than people who steal cars and large amounts of money or who run stolen kiddy rings? What possible agenda do you subscribe to that numbers this?

And just what "government" are you trying to ingratiate to your second sentence?

Dear *2600*:

First I would like to thank *2600* for their years of information. Secondly I like to see that there are those who are willing to stick up for each other in desperate times such as the case of Kevin. Seeing the web site inspired me to do a few things. I started a collect on for as many bumper stickers as I can get. My motorcycle needs a paint job so it's getting a Free Kevin custom job (the car might but it doesn't rat yet). I'm also getting a Free Kevin ramp. Soon you will be getting my order for the stickers and a photo of the tattoo (on the arm).

Gail Of Illini

You do realize that one day Kevin will be free and you'll have an outdated arm?

Dear *2600*:

You know, Kevin doesn't have the support of the entire hacking community which, frankly, surpasses me. As I was searching on usenet, I found several anti-Kevin posts, some of which suggested that he "rot until he is found guilty." I'm surprised that these people aren't outraged at how much he has been exploited - Shimomura and Markoff, both who have wanted books on the subject, have made hundreds of thousands in royalties and now, since the movie is coming out, want to make former money off of this one incident. These two bastards could be classified as the epitomes of racketeers. Kevin? Well, he has yet to make a single nickel off his story while these two sons-of-bitches are taking the story the entire six miles. Well, that's my five cents about the Anti-Kevin opinion. As far as Kevin's concerned, I'll support him 100 percent until he's released.

mek

He'll need our support well after that one of the authorities succeed in controlling his life the way they want after his imprisonment. But as we note later on in this publication, we still have much to do right now.

Dear *2600*:

Those of us in the Chicago area *2600* meeting have received an understanding: Kevin Mitnick is guilty, throw Us see in jail. While he may not be treated fairly, he is still a criminal. He got caught doing something illegal, albeit a white collar crime. If it was homicide, or grand theft auto, should you still "Free Kevin," because he isn't being treated fairly? How "fair" should someone be treated if they have 1. violated parole, 2. received arrest, and 3. committed crime after crime, never wising up enough to stop breaking the law? Kevin Mitnick must really enjoy jail, seeing as he keeps doing things to get more time. While the conditions of his release may not be so nice, he might have thought about that when he was committing 25 counts of computer and wire fraud. While I agree, you should not be in prison for three years without trial, they have a reason not to grant him bail. Bottom line, Kevin Mitnick is a felon who ran from the law, and he is getting what he asked for. If you commit a crime, you do it with the knowledge that there is a harsh penalty for it.

D-Rezz

Let's make one thing clear. You're entitled to whatever flawed opinion you come up with but you're not entitled to go around saying it represents an entire group of people. We organize the meetings and we don't have do that! Our meetings are comprised of different people with all kinds of backgrounds who hold all kinds of opinions. The one thing we all have in common is the desire to share information in an open environment.

With that out of the way, take a good look at what you're saying. You've already served as the tool and trouble of a snitch by finding Kevin guilty. Great. Now you work to your sentence. So how much time do you want Kevin to be imprisoned for? Four years apparently isn't enough for you. So what will it be, ten years? Twenty? Life? You want to equate the rather usual charges against Kevin (and they are trivial when you consider how worthless the information he was accused of possessing really is and how no damage was caused except for some bruised egos) with real crimes that deserve real penalties. His violation of supervised release was extremely debatable and/or minor yet he received a 14 month sentence on that charge alone. That time has long since been served so has the time sentenced for possessing cellular MIMs back in 1991 (eight additional months) - if growing so pissed to these charges was for only way he could be sent back to his home state of California and by the time he finally got sentenced he had already served the sentence.) So we have incredibly long sentences for rather minor violations. He was never charged with, as you say, resisting arrest. As for "continuing crime after crime," that is a very misleading and simplistic way of looking at it. When you're a fugitive, every day you remain free is a crime. What we view as a crime wave was simply one person trying to stay free and managing to do it by leading a relatively honest life, working real jobs, not stealing what he certainly could have, and simply trying to satisfy his curiosity about technology he was told he wasn't allowed to know about. You seem to believe that every crime should carry on a penalty, but a "harsh" penalty. Every instance of real hacking, every instance of computer hacking. Maybe even every jaywalker. But what is the point? Do you somehow benefit from all of the new prisons that are being built? Have you stopped to think where this attitude will get us in another ten years?

Church People

Dear *2600*:

I almost flipped when I saw my church's home page picked as the Summer 1998 issue! But I was disappointed by your choice of words (twisted reasoning, cult, etc.) which is an unwarranted slam. One thing the Bible teaches is that you should "do unto others as you would have them do unto you." Hackers get a bum rap being portrayed as diabolic geeks, juvenile delinquents, and vicious criminals when that's not what we are at all. (I say "we" rather loosely since I'm more of a hacker sympathizer; my skills are not worthy of the list.)

So I would expect the hacker community to be tolerant and not rush to judgment about other groups unfairly maligned by the media. But you post on your site a misrepresentation about what my church is all about. (Then someone who is not even a member!) and you're willing to break the law to perpetuate this misrepresentation? Listen, when people in my church buy into the false stereotypes about hackers, I try to set them straight. But now how can I convince them that hackers are cool people? They go to your site and see a satanic pentagram overlaid on the FCC web page. Not cool.

I'm sorry Justin had a bad time at my church, and if he wants to express his opinion about it, that's his business. But when *2600* provides him a stump in the name of "free speech," the downside is that it offends 96,000+ church members who might otherwise be part of the growing public support base to free Kevin and improve the public image of the hacker community.

Peter Rees says "A cultist is one who has a strong belief in the Bible and the Second Coming of Christ, who frequently attends Bible studies; who has a high level of financial giving to a Christian cause, who home schools for their children, who has accumulated survival foods and has a strong belief in the Second Amendment; and who distrusts big government. Any of these may qualify [a person as a cultist] but certainly more than one [of these] would cause me to look at this person as a nutcase, and his family as being in a risk group that qualified for government interference." (Janet Reno, *SD Mission Telegram*, 9/26/96)

So, fellow cultist, do we hang together or do we hang separately?

free radical

Harassment? Who was it who sent out a threatening letter? It wasn't us. And one word of "helpful counseling" for the conscientious pastor church was reaching out to also for what you're saying. You fail to realize that we're never referred to your organization as a cult but we have reported the fact (both here and on our web page) that others see it that way. Real big difference. You also seem to believe that the person who contacted you is the same person who hacked your site. That's nothing short of ludicrous. If we were to start doing what you guys at [xxx] have been doing with us, our lawyers might get some easy work but we wouldn't really accomplish much. And for the record, we're breaking no laws by displaying the hacked site. It's news. It's history. And it's on our site! So, if you don't like it, stop visiting it, just as you would advise people who don't like your church to stay the hell out. And finally, a word of friendly advice. If you're looking to win arguments quoting Janet Reno is not the way to go.

Dear *2600*:

HOW STUPID CAN BE A HUMAN BEING LIKE YOU GUYS?DO U WANT THE ANSWER?VERY STUPID YOU HACKED A SANT HOME PAGE WHICH SPEAKS ABOUT PEACE AND JESUS YOU THINK THAT YOU ARE INTELLIGENT BUT WITHOUT THE COMPUTERS YOU ARE NOSEING YOU HAVE TO KNOW THAT JESUS IS NOT MAD WITH YOU HE GIVES YOU A CHOISE TO REGRET ABOUT YOUR ACTIONS I LIKE HACKING AND ALL THE PROGRAMMES ABOUT HACKING BUT NOT LIKE THIS TIME TO REGRET.

Harris
greece

And heaven is going to be filled with rain?

Generic Feedback

Dear *2600*:

My letter is in response to "Brianna," who complains that you violated your own Code of Ethics by publishing "... a mean-spirited article" which provides information on "how to piss people off" and "how to make an asshole of yourself." Brianna most certainly does not need any instruction on how to make an asshole of himself.

I say that you are true to your words. When you publish letters like his, it shows you are not afraid to provide a medium where information is freely discussed and people can form their own opinions. Brianna exercised his right to freedom of expression, but he wants you to

deny that same right to others through censorship. What a pea brain he is. Information is not good or evil. It is what people do with information that is good or evil.

The more information we have, the more choices we have. The more choices we have, the more freedom we have. That is why social institutions and individuals who want to exercise control over our lives always limit our access to information.

As for those who try to "fuck with people" using information from your magazine, or any other source, I say this. In a free society I cannot control your actions, only mine. You are free to use your information to fuck with me and I am free to use my information to stop you. This is how the game is played. If you choose to play, be sure you know what you are getting into, otherwise you may end up the fuckee.

Skippie the Ageless Hippie

Dear 2600:

In your Spring '98 issue on page 33 of the letters section you respond to "Tuxedo Mask's" suggestion of a lawsuit by saying "It's nice to know your dad [a lawyer] has passed his values along to you." As you are so fond of saying in response to other letters, "you made a misassumption." Just as there is a "hacker ethic" that some hackers follow and others don't, there are ethical rules for attorneys that some attorneys follow and others don't. Just as it's the "bad" hackers who get all the media attention, you are more likely to hear about bad attorneys than the many hard working honest people who ply this trade. Since I doubt you actually know Tuxedo Mask's father, you have assumed that since he's an attorney he is unethical. You don't like it when people make these assumptions about you, and you should avoid doing it to others, whatever their vocation or avocation. There are lawyers who hack and lawyers who defend hackers in court. Unlike hackers, lawyers are legally bound to follow their ethical code, and those who don't face fines, suspension, or in serious cases disbarment. Although the ethical code varies slightly from state to state, it always includes the command to "avoid the appearance of impropriety," a catch-all provision that would include within it stirring up groundless litigation. If Tuxedo's dad had among his "values" the desire to stir up litigation he would eventually find himself in front of his local attorney disciplinary board. In fact, it would be against our code to contact a potential client as Tuxedo has to inform them of the possibility of a lawsuit. This type of soliciting is prohibited, limiting the free speech rights of attorneys in a way they aren't limited for others. Lawyers are just people with three years of law school and a bar exam behind them. These three years and exam don't change people, they empower them. Like hackers, how one chooses to use their newfound power and knowledge is up to them.

For more on attorneys who don't suck, I recommend you visit *Nth Magazine* at http://welcome.to/Nth where you'll find true stories of attorneys, the good, bad and burnt out. Thanks for putting out a great zine; I've been reading for years and hope to do so for many more.

Outlawyr

In this case, the writer made a point of saying their father was a lawyer and that we should go out and threaten to sue someone. Obviously, if that's where they got their idea, the values passed down were poor and our comment is aimed at one person, not all lawyers everywhere. If Dad does have good values on such things, he doesn't seem to have gotten around to passing them along. Our remark could then be considered sarcastic.

Dear 2600:

I recently visited America (I am from the UK) and as a result was able to purchase 2600 for the first time. Since then I have also been listening to *Off The Hook* through Real Audio. I would first like to thank you for the bullshit free information that you give and I think that your articles are top quality. I especially liked "Hacking The Virtual Pet" (14:4) - it was most amusing! I find *Off The Hook* to be equally interesting. You are the sort of people the hacking community really needs to survive.

squarechin

Dear 2600:

I am so fucking sick of this "selling out" bullshit. I've been reading your mag for a while now and I guess I must have missed the big switch when you guys gave in to corporate America and became trendy. Maybe I just don't notice the tons of commercialism packed into every new issue. I guess I'm ignorant of the fact that I'm one of the mindless lemmings who shell out millions for your mag. Maybe reading 2600 makes me a hacker-wannabe, but I like reading it. I've enjoyed every issue I've ever read and never found anything about your mag to be the least bit commercial. And so what if it is? Is it so wrong for people to make some money? I think you guys deserve it. All these super-elite hacking gods who call you guys sellouts should exercise some common sense - if you don't like it, don't read it! Calling 2600 a sellout is about as stupid as anything I've ever heard, but what's my opinion worth to such superior hackers? I may be one of the mindless lemmings who reads your mag, but it seems to me that these morons' definition of "selling out" is the mag's popularity extending beyond their personal library. It's like they get mad because someone besides them happens to know that your mag exists, and so that makes 2600 a sellout and they wouldn't dare subscribe to such a commercially controlled magazine. I'll bet they're not so damn reluctant to use the great info you guys provide. I think everyone should have the right to their opinion, but come on. Not to pour salt in your wounds, but if you guys are such sellouts, why are you having financial problems?

ecure

For the record, our financial problems have pretty much ended so we can now work on expansion and new projects.

Dear 2600:

I'm writing in response to Luke's letter in 15:2 which commented on a way to hack the Create-A-Card machines. What was described was an interesting way of trying to get in the machine if it's out of paper to try to hack the software. Here's how I do it. While the machine is running the promo screens for the different types of cards, touch the lower right hand corner of the screen (assuming there's no picture there). This brings up a computerized keypad that asks you for a password to enter the Create-A-Card management program. Great, you ask, but now what? Well, through a little investigation, I've learned that the password for the machine is usually the store's ID number which you can get by social engineering. Even better, sometimes it's written on the back of the machine. I've generally seen them in the upper right corners (K-Mart, Wal-Mart), but I guess they could be anywhere.

So what does it do? Well, after you're in, you're shown a menu that looks like 6 VB command buttons. This is the top menu to the management subsystem. The options range from printing a test card to my favorite: changing the layout of a card. You could actually go in and change the words and formats of the existing cards.

The possibilities are endless! How about a "Free Kevin" card? Just a thought...

Wraith

Dear 2600:

Your magazine makes me happy. On your latest issue, I noticed the cover artist signed "Free Kevin" with a number 4 below, a tribute to *New York Times* cave illustrator Al Hirschfeld, who signs all his work with a number below his name. The number is the amount of times he hides his daughter's name, Nina, throughout his piece. Knowing that, I found four "Kevin's" hidden on Attorney General Janet Reno after a few seconds of close scrutiny (the horror, the horror): one on her neck, two on the right side of her face, and one on her earring. It was fun. I will mention "Free Kevin" again and then go. Bye!

Kevn

Thanks for noticing but we managed to screw it up somehow. There are at least five Kevin's in there that we know of.

Dear 2600:

As I was reading "A Newbie Guide to NT 4.0" (15:2), it struck me that there are a variety of ways someone doing as the author described could be tracked down by a truly competent administrator (or even a moderately competent one aware of the problem). Since I'm not involved in administering or securing NT systems I'm sure there are a variety of methods I'm missing as well. Some of the items both explorers and admins should be aware of, based on the article in question:

1) NT has a workstation name, which I believe is logged for connections. No mention was made of changing this name, though it's easy to do if you have administrator access.

2) NT systems have unique identifiers that are not changeable, at least not without significant digging into parts of the system not often explored except by kernel hackers. These identifiers are used in some inter-system network messaging, since duplicating them was one of the problems with using early versions of Ghost to duplicate NT systems.

3) Most college networks are probably using DHCP, and if a personally identifiable system (like a laptop) is used for hacking before its DHCP lease has expired, the same IP address will be used. If the system is usually on, the DHCP lease may never expire - that would make tracking even easier. My office system's IP address hasn't changed in close to a year, despite being (theoretically) dynamically assigned. DHCP-assigned IP addresses can be manually released.

4) If the college provided the laptop's NIC, there's a slight possibility that they've logged the MAC (hardware address) and associated it with the laptop's serial number. Even if they haven't, they may be able to log which IP address is assigned to which MAC at the DHCP server, defeating attempts at anonymity that involve releasing DHCP leases.

5) If the campus network consists of multiple small Ethernet "subnets" with switches connecting them, someone with access to the switches may be able to determine what subnetwork someone is on and thereby narrow down their physical location, possibly even down to a single public room with only one person known to be technically capable - remember that your average college student probably doesn't know enough about the system he's on to realize that the system name can be changed. People technically literate enough to hack into systems are relatively rare, particularly on small liberal arts college campuses.

While most of these are unlikely to initially turn up evidence of someone breaking into a system, in the hands of an administrator who's aware of such break-ins they can be used to locate a person while the break-ins occur.

So, just as a reminder - keep in mind that using a PC OS like Windows (any of them) means that your machines are both identifiable and not used by many people, and that anonymity at the OS level doesn't always imply anonymity at the hardware level.

Alan M

Dear 2600:

Just bought my first copy of 2600 and, writer rather than hacker, I can promise you that if 2600 is having trouble getting displayed in bookstores/elsewhere, it's not because of any bias toward hacking (a displayer will display anything that sells - except magazines like *Sandy Aqua*) but because of its "digest size." The science fiction field knows this problem well. While three "digest size" SF magazines still survive (barely) and do get displayed (here and there), the new SF magazines that have made it since the 70s have all been large format. Bookstores and other displayers *hate* to display digest-size magazines; some are sure they don't sell, others just don't know where to put them. Even fancy cover art doesn't seem to be able to hurt a large format much. When you have the capital to spend, as an experiment try 2600 in large format and make *Hacker Quarterly* at least as visible as 2600. (Sorry, but I could

barely read the word "Hacker" on the Summer 98 cover and it's what sold me.) Better yet, get the conglomerate that owns you (right) to purchase a celeb's name (as one SF magazine did; e.g., *Isaac Asimov's Magazine*. *For Hackers*. Then do a Caruso and splash article teasers across your large full-bodied cover. "How to Give your Mac a Free 900 Number This Christmas." Or don't.

Mac

Clarifications

Dear 2600:

This letter was inspired by Section8's article "Hacking a BBS With DOS" in 15:1. In the absence of virus protection, the command line ECHO Y| FORMAT C: /Q/U > NUL would suffice to format his "friend's" hard drive. There are, however, a few things to note about the methods described. The above command line will cause the system to hang up when the DOS format utility prompts for a volume label. This sort of thing happens when the output from ECHO is piped to a program that prompts the user for more than one response. Since causing a system to latch up is a hallmark of poor hackmanship, one might opt to answer the volume label query in the command line with the /V:<new_volume_name> switch. For example, the command line ECHO Y| FORMAT C: /Q/U/V:LOO will proceed leaving the victim with a c:\> prompt, a volume label of the assailant's choosing, and a squeaky clean hard drive.

Another thing to note is that since most PC users have migrated to Windows95/98, the tree command will usually yield little more than an "Incorrect DOS Version" message. The better choice for interrogating such a file system would be to use the DIR/S <filename.ext> utility. Be conscious of the amount of space that will be required for the new file. If the output file is created ahead of time, it may also be of some benefit to give it a -R attribute.

One last thing. Mischief has traditionally been the way for us to hone our craft; these little attacks don't all have to leave a wake of smoking hard drives and havoc. Once security has been broken, the same methods can just as easily be used to change a stock MS splash screen to an Easter joke or public service announcement. The look on a system administrator's face who just realized that he's been violated is priceless. Use your imagination, learn all that you can, and show a little class.

Cathode Ray

Dear 2600:

In response to Mot-Falegh's article on stimulants in 14:4, I'd like to say that it was very useful information, especially since caffeine usually makes me ill in doses larger than, say, your average 12 oz. soda. It was interesting, however, that ginseng was listed as crap because of its estrogen content. As someone whose body naturally produces estrogen (read: hi, I'm a woman!), it was mildly insulting considering that your readers include those of us with ovaries. Hey, Mot-Falegh, don't assume everyone who's reading your stuff is frightened by the idea of growing breasts. Some of us already have them.

CKG

Dear 2600:

Some of the code got chopped off the end of the page at scan(!) about the middle of the page, in parse_post(!) on page 44 of 15:2 (not to mention he used a goto statement instead of a while() loop. Bleah.

Nice art.

TS

Dear 2600:

The article "secure.c" by kasper (15:2) contained a major security problem. secure.c writes to a file in /tmp (/tmp/pstab) and blindly follows symlinks. A normal user could create a symlink from any file to /tmp/pstab and when secure.c is started the program would overwrite the file. This could cause destruction of vital system files effectively bringing the system to a halt.

Anyone who wishes to have the "security" that secure.c claims to provide should look to the ulimit function provided by their operating system.

Chris

Dear 2600:

In the article "More on Military Phones" on page 8 and 9 of 15:1, there was a big mistake in the part that listed DNS Numbers. All of the numbers listed in Missouri (MO), are actually in Mississippi (MS). Bay St. Louis is actually a small, lame ass town in Mississippi, not a small lame ass town in Missouri. Do I get a free subscription?

nOhBWx

No, but you get our thanks and the pride of knowing you're aware what state you live in.

Dear 2600:

After reading Seraf's found memo "Not a Secret" (15:1) and noticing the words stuck together, I hope that you guys (yes, including Seraf) separated the word styles so they were not the same as the original message. If you don't know already, to stick words together is a common security technique to find out what message came from who over a dissemination process such as a public news broadcast or newspaper quotation where the original letter would be shown. For example, group A gets the memo with the words JaneDoe stuck together while group B gets the memo with the words Jane Doe separated by a space, group C getting Jane Doe with two spaces in between, group D getting jane Doe with the j character in lower case and the d in upper case, etc.. If this procedure was taken from the originator of the message and the message was printed exactly character per character, such as from an OCR (Optical Character Recognition) software program (OmniPage Pro, TextBridge), and the software did not have any modifiers to change such above said, then the group or individual who either gave the information or who threw it in the wrong "memory hole" has either probably had a talking to, or is being investigated even further. This style and technique vary from words stick, to extra line spaces, to off indentations, to bogus paragraphs, to typos. The key is to make the same letter appear somewhat similar, but different enough to identify the "mole." Also, this technique is performed to weed out the moles in a high security situation concerning information warfare.

GZRaXAX

We'll never tell...

Dear 2600:

I had to write in to point out the errors and miscellaneous lameness in Friedo's "CGI Flaws" article in your Spring issue:

1. CGI is not inherently "flawed" because it runs on the server-side. It isn't practical or desirable to transmit large databases to the client so that they can be processed on his/her machine. How many search engines do you know that aren't server side applications?

2. In the fake ls script, what's "copy"? We're on UNIX, not DOS - try cp...

3. What are all the extra ";"s for? These have no effect other than requiring extra typing.

4. Why does the fake ls script run the real ls with no arguments??? Your ruse will be discovered pretty fast if the sysadmin uses ls -l or something. The script should say "ls $*".

5. The fake ls won't be executed if the sysadmin has "." anywhere in his path! It would have to come before /bin and /usr/bin. If the sysadmin has "." in his $PATH and it doesn't come last he is very stupid indeed. This is the first commandment of protecting yourself (and your system) from your users. Besides, this old trick really has nothing to do with CGI!

6. Friedo says to make .somebinary perfect before you pull the suid gag. Not very flexible. Why not have .somebinary call .someotherbinary? That way you can change .someotherbinary to do whatever you want.

7. SUID does indeed work on scripts on many/most UNIXes, but not with csh - try sh or ksh. On some UNIXes you need to use something like "#!/bin/sh -p" to have the system preserve the effective UID.

The "Setting Up Unix Trapdoors" article in the same issue was much more on-track, though there's one glaring problem. All of the ">"s should be ">>"s! Otherwise you're wiping out /etc/services, /etc/inetd.conf, and /.rhosts. This will no doubt blow the system out of the water - not very discreet.

Also, the hint to system admins to search for suid programs with a modification time later than a certain date is not very helpful - timestamps are trivial to fake. diff is also unreliable as you'd need to be diffing against backup copies of the suid programs, which the hacker will have found and modified if he's worth his salt. Therefore, it's best to compare checksums. Hardcode them into an executable so the hacker can't easily just change them to the new values. And don't call the executable compare_suid_checksums - make it something innocuous so the hacker won't know to monkey with it.

Whirlwind

Dear 2600:

nathan@senate.org's article "setting up unix trapdoors" has some errors in there that are very misleading to unix newbies.

I contacted the author and he says he typed things right, and I believe him. Just a reminder to your editors and authors I guess that ">" is very different than ">>".

The lines echo "tcp 2600/tcp # Network Security Protocol" > /etc/services and the associated line in inetd.conf will replace these files as we all should know. And you don't want to do that. Using >> instead will of course append those lines to their respective files without overwriting them entirely.

emory

This was a mistake that occurred on our end during the layout process and probably one of the worst we could have made. Ironically, it was a computer error. We're sorry for any problems it may have caused.

Dear 2600:

Vandal's article in 15:1 titled "ANI 2 - the adventure continues", is incorrect about five things.

1) ANACs using ANI II have been in existence for a while. Over a year now, actually. So they haven't been "popping up" as vandal suggested. On the same note, ANI is not ANAC. There is a difference.

2) The call letters used are not Greek letters, they are phonetic letters. "Charlie" is not a Greek letter (as read off by the dead 800-555 ANAC).

3) The ANI II digits are read out before the number, and then only on ANACs that are owned by MCI.

4) The list he provides is not every known ANI II code, it's every possible ANI II code. (He should have read the damn thing first.)

5) The 07 code does not signify an operator assisted call. The 07 denotes that there is some type of restriction on that line that prevents calling. For example, you are at a COCOT and you call 1-800-487-9240. It reads back all of its information and then says "ANI number: 0,7,6,1,4,6,3,4,9,3,7,6". Perhaps that COCOT has an international calling block, or a 900 or 0700 block. Another example: you are in a condo rented by a resort (as in you are not on their PBX). You call up the ANAC, and it tells you that your ANI II digits are 07. Maybe that line has a restriction that prevents it from dialing out of LATA. Or maybe you can't call directory assistance from that phone. Just for the record, the normal ANI II digits for an operator assisted call are 34. Check for yourselves.

On a different note, while many of the RBOCs have stopped giving you a dial tone after one side hangs up, SNET (Southern New England Telephone, the reigning LEC in Connecticut) is still doing this! Remember the easy days of ripping pay phones off by letting 1-800-LOAN-YES hang up? It's still possible there! Oddly enough, it seems as if some of the countrywide COCOT providers are unaware of this. Today (7/17) I was at a COCOT that was manufactured by Elcotel when I found this out, coincidentally. I called up an ANAC to add another pay phone number to my collection, and when the

letters continued on page 48

SCREWING WITH BLOCKBUSTER VIDEO

by Hiemlich VonScooterraus the 53rd

The corporate invasion is well underway now. By the time you read this, Viacom will have stuck a Blockbuster store within earshot of your house. A boon for many, a curse for many as well. Having worked at a franchise that was bought out by the corporation, I can honestly say that things at the local video store are going to get worse before they get better. Corporate stores are now the norm as no franchises are being sold anymore. This ain't good. I'll explain why by dividing this article into two parts, the first being:

Franchises

OK, for those of you who don't know, a franchise is a store owned independently of the corporation that owns the name. So, a franchise Blockbuster would be owned by Joe Schmoe, and he would buy all the movies, distribute pay checks, and reap the profits. A corporate store is owned by the corporation and they do all that stuff themselves. That being said, it's pretty obvious which type has to put up with less red tape.

Speaking as an employee, I can tell you that once my store was bought, we were immediately forced to watch some dried-up film star tell us how to deal with robberies, how to prevent theft, how to exit the store, how to breathe, and how to eat. Big time brainwashing. One of the things they didn't mention, however, is what to do if presented with an account that seems fake. All the better for us, the scorned few.

Here's how Blockbuster rents you a movie. They ask for your card, or, lacking the card, ask you for your driver's license. Also, you can quote off your account number and use that. So, if I were to say my account number were 2580011378, the loser behind the counter (who makes minimum wage, by the way) would type that number in and see all my info. So, if one were to say, run in, grab a copy of *Road Rash 3D*, a copy of the MS13K movie, and a copy of *Breast*, they could give the counter person the account number of the guy who used to take away their lunch money in second grade, pay rental fees, and have a bigger movie collection than when they went in.

Alternately, one could feasibly, sift through the dumpster behind Blockbuster and find a membership card that was misprinted and thrown out, get it laminated (or just memorize the number on it), come back and use it. At no time does Blockbuster check ID if you present them with a membership card or a membership number. There are pitfalls to this, as some accounts can be rigged to say "Check the ID of whoever uses the card" but that usually only happens when someone loses their wallet.

This works at both franchises and corporate store by the way.

But, as I said, some things won't work at corporate stores. At a franchise, for example, they use these little cards to scan in discounts. If I return a red-covered movie and ask for the dollar back, a franchise store has no way of knowing whether or not I actually did it, they just take my word.

A franchise is a lot more lax about security too. I can say from experiencing two separate franchises that their video surveillance systems are complete wastes. They have three months worth of videotapes in the back. Each one records *24 hours of activity*. These are normal tapes!!! Hah! Even brand new, these things are unusable. One time, a customer was bickering about whether or not he rented something, so we took him back to show him coming in the day before on the tape. The tape was so stretchy and mottled, we couldn't see a thing, so he got his money back, and a free rental to boot.

Which brings me to the next difference between corporate and franchise: franchises are tougher to get money out of. That being the case, lets move on to

Corporate Stores

A corporate store has one goal: give you, the customer, whatever he or she wants. You could walk in and have $100 worth of late fees on your account, and if you make a big enough scene, a corporate store will always give in and apologize profusely. No kidding, you can get out of late fees as much as you want, just bitch and moan and complain.

Corporate stores, however, spend a lot more bread on security cameras. When we upgraded, we got a top of the line video monitoring system, even if the only cameras were trained on the checkout, leaving shoplifters to grab anything without a magnetic tag on it.

Corporate stores also keep track of their discounts. They don't just hand them out, they actually keep track of them on their computers! Amazing but true.

And what about their computers, you ask? Well, my friend, this is where it gets tricky. The good thing about the computers is that Blockbuster runs some freaky system that keeps them constantly locked to every other Blockbuster in the world. Yeah, that's right, I can go to Dallas tomorrow, tell them the account number of my old boss, wait 30 seconds, and leave 35 bucks poorer, but 5 Playstation games in the clear. Ain't it cool?

The downside of this system, however, is that you can't get away from late fees. (Unless you piss and moan.) If you have a late fee from another store, there is dick-all a new store can do about it. Oh sure, they could take it off, but company policy is not to do crap to members from other store's account fees.

The Blockbuster computer systems themselves are an enigma to me, as I'm not particularly adept at odd systems. I can tell you that they run on PC's using an independent operating system, so there's no dropping to a C prompt. To log into one of these things you need the last five digits of an employee's account number and their password. The passwords are over four letters, so you can work at it, but I have yet to find a store where the computers are easily accessible. If you do get a shot, try simple passwords. Most people who work at Blockbuster wouldn't know the difference between DOS and Windows, so they're generally morons when it comes to passwords. At my store, during a boring night, all the employees gave away their passwords, if you can believe that. Smurf, Booger, Titanic, stuff like that. Once in the system, you really can't do anything useful unless you get a manager's password and number. Ok, account numbers are generally kept on a list with names somewhere behind the counter, so getting a number is relatively easy.

OK, let's say one has managed to get a manager's account and password. You'll see a prompt. All you have to do is either scan in a membership card or just type in the whole 11 digit account number and hit return. Bingo, you've got the account on your screen, including balance due, number of movies rented, etc. etc. So here you need to look at the keyboard. F11 clears the account. F10 goes to the check-in window. F6 (I think it's F6, but most keyboards have idiot stickers along the top that say what the F keys do) should be refund. So, let's say I got my account up, with no balance. I hit F6 and a list of refund types comes up. I hit the number of the item that says "credit." It asks for validating number and password (your stolen manager's number and pass) and I type them in. Now, I type in the amount I want back. Note here, what you type in should be a factor of 3.66 or 5.24 as these are the rental prices of new movies and games, respectively. If the amount is something other than that, the goober behind the desk might get clued in.

Bingo, you're all set. That's about all I have on the subject for now.

Screwing With MovieFone

by thirdhorse

MovieFone (MOFN) is a publicly traded company that lets you purchase movie tickets with your credit card via the phone or their web page. Known as 333-FILM in the Boston area and 777-FILM in New York it is available in 30 major cities and serves 12,000 screens. MovieFone has ATM's in the lobby of all theaters it services. Each ATM has its own CPU, screen, printer, and card reader. They come with a test card which when slipped in and pulled out produces a ticket that says "TEST" on it and nothing else. The ATM's use a LAN (Local Area Network) to connect to the theater's management computers.

MovieFone has many uses beyond simply buying tickets.

One of the most obvious is getting into R rated movies if you are under-aged. Buy the tickets via MovieFone and no box office person will ID you.

MovieFone used to accept any expiration date so you could use a generated credit card number, but nowadays it requires the proper expiration date. This can be helpful if you find a number somewhere but no expiration date. Simply hack it out via MovieFone by advancing month by month until you get the right one. If you tried something like this on an LDC (Long Distance Carrier), the card would be blocked from making calls through the carrier even with the correct expiration date.

So you got a card number but no card? MovieFone ATM's require the use of the magnetic strip on the card via the card reader and has no options that allow manual input of the card number. However since the ATM's are on the LAN of the theater's computers, tickets for MovieFone can also be picked up at the box office where those terminals do allow manual entry of the card number. All you have to say is "I left my card at home but I have the number, can I still get my tickets?" One would think that the box office people would be suspicious, but they never are - it happens so often.

This technique can be used by box office cashiers for getting extra cash. Before their shift in the box office or while on break they order tickets using stolen credit card numbers. The four ticket per transaction limit MovieFone has installed is no good as you can call back using the same number to again purchase four more tickets. The employee then punches up those tickets while in the box office and sells them pocketing the cash. It is safer than selling courtesy or discount tickets at full price as MovieFone tickets printed at the box office are identical to tickets purchased with cash.

Anybody else could also refund the tickets for face value in cash. This only works if you get the tickets from the box office because when you get the tickets via the ATM's they are printed differently and cashiers are not supposed to give cash refunds for those. But you can still get passes.

Using your own card it is possible to order and pick up tickets which you then give to your friends. Then you go back to the ATM to "try" and get your tickets. When they don't come out ask to speak to a manager or somebody who can help you. Explain how you ordered tickets and waited for the confirmation (most people who don't get tickets don't realize that they have to wait for the confirmation) but the machine says your order is not found. The management will check your card number on their management station which will show that you were charged for X amount of tickets. No MovieFone or theater computer is able to tell if the tickets were picked up or not. Only the time the theater received your order, number and type of tickets purchased, your credit card number, and the name of the movie is recorded. They will walk you and another group of friends in so that you can join your friends already in the theater.

The management's station keeps a list of all credit card numbers used. During a busy weekend day you could pull up 500 or more credit card numbers. For instance, at Sony/Loews theaters they use the Prism Theater Management System. From the main menu you click on "Daily Operations" then click on "Credit Card Management". The first selection on this screen is the one they use to see if your card has been billed. You enter the card number and it searches back up to three months (default is 14 days) and lists the tickets you bought. The other or second selection on the credit card management screen will give you a list of all credit card numbers and other information previously listed with an option to print to screen or printer. Prism puts 36 card numbers on each page. When going to this screen it sometimes says "Error" but just click OK.

Even after you use your own card you can call MovieFone for a refund at 800-743-0009. Tell them you never went and picked up the tickets or that you want to know what this charge is as you have never used MovieFone in your life. (You can also call 800-745-0008 to *change showtimes* or perform other managerial tasks.)

There are many other uses for MovieFone, like using it as a DTMF Decoder but this should give you a basic idea of some of the possibilities.

For more information from them email info@moviefone.com or check out their web page at http://web18.movielink.com/

Screwing With Radio Shack and Compaq

by Informagnet

Well, Radio Shack's firmly in bed with Compaq. This ends, for at least a while, their selling computers I have some respect for. This article should clarify why I say this.

While Radio Shack was selling IBM computers, there were actual working IBM Aptivas out there on the counter for the customer to play with. These were password protected to prevent mischief, and the protection was at least good enough to keep the machines safe from types like myself. I couldn't even get to the desktop with a hit-the-power-switch cold boot; the machine would just go straight to its demo with no "side trips" allowed. The only way I could see anything but IBM's excellent demo was to SE the password, (default was "merlin") and when I abused this trust by changing the password, I was greeted the next day by the amusing sight of the manager preparing to take the cover off of the machine so that he could pull jumpers. If there was a "backdoor," even he didn't know it, and Tom's pretty computer savvy. IBM had set these machines up with pretty decent security, and having bought one, I am still very happy with the "seamlessness" of the software.

With the invasion of Radio Shack by Compaq, things have changed to a hilarious degree. My local Shack has three Compaq models on "display." Actually what one encounters is three empty cases with the keyboard, monitor, and mouse connected to an actually operating computer locked inside the podium the display dummies sit on. This arrangement is for security. There is a "hard and fast" policy against letting even favorite customers know the password, so this has got to be much more secure, right?

Well, after 15 minutes or so of simply trying random stuff, I found a backdoor that even the most paranoid manager can't shut by changing the password. Compaq is going to be overjoyed to have *this* become common knowledge! I found that there's a flaw in the demo that makes it possible to get to the task bar, and from there do anything you want. It seems that the computer is responsive to keystrokes for a very small time window while it changes from one demo subprogram to another, especially when you are several steps in and then click on Home. The procedure I found to consistently work was to click on "click to learn," then on one of the computer models (I always use the highest one), then going to the surround sound demo, then the game, then as the game starts, clicking on Home. During this time, hit Control-Esc and you'll get the task bar for just a moment. It's sort of a flaky process, sometimes you'll see the task bar and the game screen both, each sort of transparent! You have to move quickly and if you miss it, just try again. It's a matter of getting the machine busy and then "getting in a command edgewise." But it works. I was hanging out "helping" close up the local store one evening and was able to shut down all three machines in a few minutes, impressing the guy there enough to tell me the password, "RS2C98." Remember, when trying this, those caps are important, and don't hit enter after typing this in, as this is counted as an extra "character," just click on the action you want to do on the menu. I think this is a nationwide default password, at least for the Shack.

How does this "side door" work? My theory is promising - these new Compaqs are all Pentium II machines. As flaky as the programming of these may be, basically they can eat multitasking for breakfast. When I am getting into the task bar and DOS prompt, the machine is multitasking, running the demo *also*. In fact, if you don't keep inputting keystrokes, the machine will go back to the demo! This can actually be useful when you are getting glowered at. What makes this "promising?" Well, this points out a strength of the new generation of computers coming out now and a weakness in people administering them, who tend to have cut their teeth on DOS machines that were much weaker in their multitasking abilities if they had them at all. There's a good chance that a lot of things will be possible to get into before admins really learn how to secure a PC system with multiprocessing capabilities rivaling supercomputers of just a few years ago.

So, what do you do with this knowledge? Well, not all Radio Shacks are staffed by cool people like my local one. Some of them are full of real jerks. Jerks, especially jerks with no sense of humor, are the enemy, remember? Keep in mind that humor is the weapon of choice. There are HTML training files in there that clearly benefit from a little creative spelling like "antinnuh" for "antenna" and so on. Or, you may want to experiment with effects. Of course, you can run two demo program processes at once. You will hear the audio of them both, and they will not be in sync. Wowwwwww, weird echooooo.... Now *that's* an effect! I must admit, the top-end model's sound *is* impressive, and this makes it sound like my favorite band, EBN. Imagine how some grumpy old Radio Shack manager's attitude will improve after *this* type of musical enlightenment! I didn't get around to trying more than two demo programs running at once, but I'm sure you can run several.... Between the flaws in the demo software and what I see as a general flakiness of the machines themselves, much entertainment and experimentation is possible. Even after Compaq gets the idea there's something wrong with the demo and gets something more secure out into the field, there's the basic instability of these budget-built machines.

I have noticed that CostCo has these Compaqs too, but wasn't able to get any experimentation in the last time I was there because the one there was locked up *solid*, and I mean catatonic.

Some general tips on Radio Shack. Trashing there can yield store number and employee numbers. These of course can easily factor into passwords, as with any large corporation. There are employee training and testing files on whatever is the favorite Compaq - they are fun to look at. The Shack is a good source of batteries, being able to get you just about *any* battery, and they are worth being on good terms with. Their latest 65-721 programmable tone dialer is the most experimenter-friendly one I've seen (remember, redboxers, the crystal is the little yellow thing that looks like a capacitor). In general, I think the quality of Radio Shack products has improved a lot, and it's a letdown to see them take a step backward in the computers they offer.

Want to send something to *2600* and make sure it's private? PGP it!

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.0

mQCNAjsAvogAAAEEAKDyMuRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIo34Jr10u9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI1G8nR0RB4J8Rwd+tMz5lBKeK19LzlSW1R
hLNJfm8v8j7Hd8nQBen3794wWWCyEpoqzovu/0UthMLb6U0PC2srXlHoedr1AAUR
tBZlbW1hbnVlbEB3ZWxsLnNmLmNhLnVz
=W1W8
-----END PGP PUBLIC KEY BLOCK-----
```

trunking communications monitoring

by TEL Egodzilla

The powerful marriage of computers and radio communications created a new child of the 21st century: *trunked radio systems*. Trunked radio communications allot multiple users to all available channels/frequencies through a series of user programmed controls. Conventional radios traditionally limit user access to their assigned channel grouping (channel 1 to repeater 1, channel 2 to repeater 2, etc.) whereas trunking affords full implementation of all available channels' frequencies at any given moment while yet allowing full system programming. Note how the term "trunking" is used – it's from (you guessed it) telephone trunking.

In trunking, "talkgroups" (groups of radios programmed to speak to one another) are the norm. Individual radios are programmed via a typical PC (usually a laptop to allow for ease of portability). Each trunked radio holds a computer chip allowing for a "personality" programming. Groups of radios can be programmed by creating "profiles" - usually in minutes - and rapidly duplicated or, if need be, individually tailored. System users thus better employ the number of channel sets their overall system employs. In many instances, a typical trunked system can carry over 2,000 user-specific talkgroups allowing for several hundred radios to be assigned to each individual talkgroup.

Trunked communications employs precision computer control, enhancing system efficiency. Trunking controls re- when and for how long each user can talk as well as the priority each user possesses. "Dumping" or "crowding" is far less likely to occur on a trunked radio system than any other and waiting time is dramatically reduced. Users are "queued" and stored in memory. Users with higher priorities are enabled to be put on the air quicker than others (based upon how the radios are programmed) while data communications (depending upon the model of the system) functions on background operations.

Trunking also allows a system overseer to turn off a (or several) radio (s), should it/they become lost or stolen. When recovering a trunked radio, enjoy it while you can: it generally doesn't take long for that radio to become a useless paperweight with the flick of a remote switch at the System Controller.

Security is enhanced. Digital trunking systems enable full digital communications, censoring against eavesdropping. Depending upon the make - Motorola and Ericsson are the two top contenders (E.F. Johnson also makes a conventional trunked system, but they're having problems with their design) - there are different approaches and points to consider.

Motorola: Smartnet and Astro

Motorola's two primary trunked systems - Smartnet and Astro - are worlds apart. Smartnet is junk; a recent State of Hawaii court ruling illustrated that Motorola's Smartnet is not, as so defined by trunked communications requirements, a true trunked system (which goes to show that when buying Motorola, stick with their pagers). Agencies using Smartnet can be readily breached via a typical trunked scanner (also known as trunk trackers). Some recommended models are the Uniden Bearcat BC235XLT (handheld) or BC895XLT base scanner) - assuming that the Smartnet system in question is actually functioning. There have been a growing number of localities who've had their Smartnet systems ripped out and replaced.

Astro is a tougher nut, but not too many organizations use this system as Astro is expensive and is non-compartmentalized; in other words, when you buy an Astro, you gotta buy everything at one time. Unless an organization has a couple of million to spend every time it needs to upgrade or expand, this is not an economically viable system to obtain.

Ericsson: EDACS

Ericsson systems are choice: if you want a good, reliable system for a decent price and one that'll keep out the weirdoes, get an Ericsson EDACS system. EDACS (Enhanced Digital Access Communications System) is used by the Secret Service Presidential Bodyguard as well as the U.S. Navy's Carrier Strike Force's ship-to- ship communications backbone, and is currently used by Boris Yeltsin's bodyguards. EDACS has been used in Bosnia by U.S. forces as EDACS is truly military specs, designed to be tossed out the back of a C-130 (via parachute, of course) and ready to be deployed in minutes. EDACS can also be readily enhanced for specific parts or services; one need not buy an entirely new system when you get EDACS.

Ericsson systems use AEGIS encryption. Forget about trying to crack AEGIS; it's NSA (National Security Agency) rated and unless you get heavy iron with massive power and time on your hands (and I mean *lots* of time), you ain't gonna crack it - period. It's not surprising that the feds are always assigned at least one radio to keep their hand in the action, no matter how small or insignificant the locality's trunked radio system is. Don't waste your time - it's not enough to obtain the algorithm as AEGIS is fully digital and unless you have full physical access to the System Controller, you can't listen in.

Trunked radio systems dedicate one frequency out of their total set for the control channel; this control channel constantly transmits each and every transmitter/receiver's own unique programming, thus locking out anyone from "stepping" on the frequency set. If you do tune into the control channel, all you'll get is a rapid sledgehammer sound effect and quite possibly a fused speaker (and headache) if you have your volume up too loud. Accessing it won't do you any good.

All is not lost, however, as encrypted radios are not cheap - they usually go for about $2,000 apiece; most private and public entries, therefore, use the regular unencrypted communications - allowing listeners to employ trunk trackers with no problem. When monitoring trunked systems, remember that you first need to know the frequency set that the system is using. This can be achieved by contacting the FCC and obtaining a listing of frequencies that are being used - this is, after all, public information. Other frequency resources to consider are the Pocket Guide series of frequency directories for selected portions of the United States (contact point: *Scanner World* at 518 456 9609). Trunked trackers can be readily purchased for as little as $150 on up – if not cheaper. *Make sure that the frequency set you wish to check out is current on the tracker of your choice.*

Some systems will defeat the trunk tracker, however, by setting up a "tail" - the end of the communications broadcast - to hang a second or two longer; this confuses the tracker and makes it hard to listen in on the action. Many radio managers don't do this kind of thing as this, however, would involve prescience and intelligence on the part of managing a radio system. As with most hierarchical structures, radio controllers tend to be awarded on the basis of obedience and trust – not necessarily of intelligence and initiative.

Utilities (read: telephone), oil refineries, airports, police, fire, and paranoid private/public security forces are among the primary users of trunked systems. Trunking enables system deployers to request a minimal number of frequencies which, through the enlightened vision of our FCC, often costs a lot of money or requires a tremendous waiting time. There are also conventional trunking systems which piggyback onto regular radio systems; a typical trunk tracker can, however, handle these with no problem.

In an upcoming issue, I'll discuss more about selected aspects of trunked communications. Radio communications carry a lot of information and trunked systems are the coming wave!

letters continued from page 39

ANAC hang up, it clicked me to a dial tone. At first I assumed that it was the COCOT's fake little "I mute the handset hahaha" dial tone, but to my surprise, I dialed a test number in 212 (from 201, mind you), and it connected me without any problems, and without my lovely dandy tone dialer. Oh, and the mouthpiece wasn't muted. As odd as it may seem, this phone even allowed international calls, and country direct operators will connect you and "bill it to your number," so long as the ANI II codes are "00".

And I immensely enjoyed the article about phacking. It made me laugh for an hour. Keep up the good work.

MMX Killa

Curious

Dear 2600:

I have no doubt that hackers are being targeted by the government and I have no doubt that the government is afraid of them. Hackers now know how to do everything from hacking Best Buy to crashing *Pentagon* electronic communications, but I have a question. Why doesn't the FBI or the NSA just shut your mag down? If you're such "a threat" to national security, I would imagine that the Pentagon would send out a SWAT team and raid your place, guns drawn.

Skeet

Even those people who think we're more of a threat than drug-dealing satanic pedophiles would see the danger in shutting down our printing presses. It's a First Amendment kind of thing.

Dear 2600:

The WIPO treaty seems like it will become law with no problem. Will this be the end of 2600 and other hacker related publications. Do you have any alternatives for 2600 without deviating too much from the intended theme?

Neurotik

What upsets us most about all of the stupid laws and bills that seem to have no limitation is the apparent willingness of people to obey them. When a law is unjust, you have an obligation to challenge it. Not just in the courts but in real life. The latter is really all that matters in the end anyway. (We should stress that you need to really believe in what you're fighting for before getting involved in such an effort.)

Numbers

Dear 2600:

Thought you might want to know some of this.

I recently found some fun (though not too helpful) numbers in the DC/MD/VA area. If you dial "811" in the DC area or the MD area - you access some ANI service. You'll get the number you're calling from. If you dial 958 and the last four digits of the telephone you are calling from you will hear a pause. Push down the receiver (without hanging up) and you will hear a beep, hang up. It will call you back about 10-15 seconds later. This also works from pay phones, but not COCOTS, just Bell Atlantic phones for some reason. Used to work in Chicago too, so maybe it works elsewhere? If you dial (202) 362-9905, you will get a computer message saying "Hello I'm SSCU, your identification please." Enter the phone number of whoever you want to call and hit the # key (once to hear it read back to you, twice to hang up). It will call that number and say "hello" for as long as whoever answers stays on the phone. (Not much use except to annoy people since *69 will lead them to that number...) Oh, and of course, it won't call long distance. Any clue what SSCU might stand for?

Infect

We're asking.

Career Move

Dear 2600:

I need to find a place where I can buy one of those tools that the record stores use to take those big plastic things off the CDs. Is there any place where I can buy one at. Also, I need the tool that department stores use to remove the ink bombs from clothes. Please help if you can.

triplogik

Go to your local precinct and ask the guy in the big tall desk to hook you up. Don't take no for an answer. You may have to ask a few times before you advance to the next level.

Surprised?

Dear 2600:

It was announced on *Dateline* on Monday, July 27, 1998 that the Secret Service has a list of 50,000 people that they monitor and 250 people that they actively monitor as a threat to the government. They tag their credit cards and set up surveillance following them around, but what is even more shocking was their admitting that they bugged the people that they actively monitored.

KB

They probably don't realize it's bad.

Questions

Dear 2600:

While dialing an ex-girlfriend's number repeatedly (she owes me dead presidents and is running), I stumbled on an interesting phenomena. After about eight times of getting her voice mail, the number would come up busy or I would get her busy ("I'm on the phone right now") message. Then after another try or two I would get a strange dial tone and then a partial playback of a voice mail message. It lasted about 10 seconds and I assume the message was hers. After the message ended I would get disconnected. I tried back several times within a two day period and always heard the same partial message playback. It happened five times and from different phone numbers. At the dial tone and during the message, pressing keys seemed to have no effect.

She is in the 201 (Northeast NJ) area code and subscribes to Bell Atlantic's Home Voice Mail. I am pretty sure that dialing the number repeatedly overloads the switch. I wonder if the overload could somehow give me access to more messages or perhaps the entire voice mail box or beyond? Let me know what you find out.

RepoMonster

We find it very unlikely that you could single handedly overload the switch by calling back eight times in a row. What probably happened is that your mailing victim, while in some sort of a panicked state, tried desperately to make a different outgoing message to maybe hide her identity, failing in the process. Either that or she deliberately did this in order to confuse you, which she again obviously failed to accomplish.

Dear 2600:

why can u not answer??! how can i get in touch with someone who can answer my question about hacking into a schools computer and changeing your grade.. i will subscribe to your cool magazine if u can tell me how or who i can contact to get this information.. well thanks for your time...

VaPLaToNiCM

Just one of many lamebrains who gets into arguments with our e-mail auto-reply that says personal replies aren't possible.

Dear 2600:

Do you guys consider cartoons? I have some that I bet you'd like, but I don't want to waste anyone's time, so please let me know if you'd consider them, and how you'd like to receive them.

Nathan Hendler

If it somehow fits into what we do, go ahead and send it in. If years go by and we don't use a single one, that's a tip that they don't fit in.

Dear 2600:

I just love your webpage it's kool. i wanna get the 2600 magazine . i don't really understand what you do. are you hackers or what?

Malbasha

Oh no. We're not falling for that again. You folks think you're real clever, don't you?

Dear 2600:

I was wondering if Berlin counts as a former Iron Curtain place, and is therefore entitled to free subscriptions?

Arag0rn

Since you guys got swallowed up by a Western country, we have no way of differentiating the West from the East. So sorry, you don't qualify. But everyone else in the former Soviet Bloc does as does Cuba and all of Africa except for South Africa. But to get your free subscription, you must mail us from your home country! No e-mail, no third parties. If you can't take the time to do this, we can't help you.

Incidents

Dear 2600:

I am 16 so I go to school and of course we have computers and the typical sysop who does not even know how to create a directory but she called my parents and said she would call federal, state, or local authorities if I did not quit my "hacking." My so-called "hacking" was using the Novell send command to broadcast the message "These Machines Suck" to every computer in the school.

Nat X

Yeah, a federal crime. Right.

Dear 2600:

I was recently investigated by the FBI for scanning some systems in Australia for common exploits using a program called mscan. Anyway, that isn't important. What I am writing about is the Kevin Mitnick deal.

When I got Volume 15:1 of your zine, I also received a "Free Kevin" sticker. Being the good little hacker that I was, I went around looking for a very public place to stick the sticker where it would reside for some amount of time. The sticker seemed to go great with the dark blue paint on my uncles piece'o'shit truck, so I stuck it in the back window (I don't drive yet, so I had nowhere else to put it).

During the time that the FBI spent at my house questioning me (and taking my things, which at the time of this writing, I have yet to get back), my uncle made a point of showing the FBI that he was ripping off the "Free Kevin" sticker, and throwing it in the garbage can. This pissed me off severely.

After that, the FBI agent involved spent about 30 minutes telling me how no one supports Kevin Mitnick, and once a hacker gets busted, none of his "hacker friends" stick behind him. He also told me that the people at 2600 had no support, and that they had only been able to raise about $200 for the defense fund. He also backed this up with the statement that no one cared about me, and wouldn't support me if I ever went to jail for hacking (something I don't plan to do anytime soon).

The main point I am trying to get at here is that the support needed by the public isn't getting there because of fear. The FBI struck the fear of God into my uncle just by being there. He thought that because they would see the sticker, they would label him as a hacker and

therefore "blacklist" him for the rest of his life. I am sure I am not the only one who has seen an incident like this one.

darapleX

Unfortunately, this is a common reaction among many people. It's wrong to blame them for this however. Nobody knows how they're going to react to the threat of governmental retribution. The mere prospect really scares the shit out of lots of people. They are not below average for failing; you are above average for succeeding.

Dear 2600:

I live in Hoffman Estates, Illinois about two miles away from Ameritech Corporate and Technical Institute. I was riding my bike and saw the security gate was up (very rare). So I got in and looked around. I thought I might find some discarded manuals in the trash so I drove around the damn thing four times before I saw a bunch of smoke down the road so I rode down there and there was a monstrous incinerator. So I thought I'll just get the hell outta here and then I saw another Ameritech building (the institute) so I rode over there and wanted to get in so I walked up to the doors and they were locked so I asked the guard if there was a phone inside I could use to make a local call so he let me in. He pointed to a corner and told me to use the phone and then leave. As soon as he turned his back I walked into the cafeteria and into some sort of room that had a steel door with a camera above it and two armed guards. I turned around and four unarmed guards were staring me down. The taller one said "Come with me." So I followed him and he took me outside where two real cops were holding the patrol car door open for me. To my amazement they already had my bike in the trunk. I thought they were going to take me to a police station but instead they took me to a building at the headquarters. Inside they questioned me about where I was from and if I owned a cellular phone or a beeper. Then they took my fingerprints. They told me to sit in the chair while they called my parents and ran my record. I overheard a man talking on what looked like a beeper sized phone to someone. I heard him say that I had talked my way into the public office then snuck into the cafeteria. Then he told him SCAT-9 wasn't touched. So my parents picked me up and three days later my parents were told that an Ameritech Security Manager and a law enforcement man wanted to have a meeting with me. They came over to my house (with my parents' permission) and drilled me about my interest in phones and computers. The man from law enforcement identified himself as a computer security investigator and asked me if I had been out of the country or was planning to be. After the meeting the computer security guy told me that he would be watching me. For the past two months I have had a car outside my house (a Lincoln) and hear unusual clicks on my phone line. I sent an e-mail to my friend to ask his dad about it (he worked at Ameritech). So two weeks later my friend called me up and told me that his dad asked around at work about SCAT-9. He was intensely questioned about where he had heard about SCAT-9 and almost lost his job. He was questioned by a man and all of his files from his file cabinets were missing. So my question is what the hell is SCAT-9 and who is across the street from me?

darkrazor

Assuming you didn't somehow morph a video game into this adventure, we'll try and get to the bottom of it.

Dear 2600:

Today we started school here in Salina, KS, and after being late for desktop publishing and getting made fun of by the seniors, I sat down and pulled out my binder. Shortly after pulling it out of my bag, the teacher noticed a flyer I put in the clear pocket on the front for the cover of the binder. The flyer was one I printed off that protested Miramax making the movie *Takedown* portraying Kevin Mitnick as an evil violent hacker. So as the teacher read the flyer, I kept thinking to myself, "I'm gonna get suspended for this one!" but as it turned out the teacher thought it was interesting! She said one of the assignments was to make a school newspaper and she told me to make an article on Kevin Mitnick. I will send you a copy when I am done. Just thought I'd let you know I'm spreading the word about Mitnick.

SkidMarx

It's sad when kids in school are afraid to express themselves for fear of punishment. We're glad it worked out in this case.

Dear 2600:

So I was fired from my job today. I was working at this Place called Consumer Card Services (1-800-551-2781). It's based in Oklahoma, but I was working out of the satellite office in Phoenix.

Anyhow, what we sold was financial backing on credit cards. We had a list of rebuttals and if the people were to ask "how would people get my account information?" the response I was supposed to give was, "Well, Mr/s (blank) maybe you've seen this on the news lately, but there are malicious computer criminals called hackers who will stop at nothing to get your account information so that they can make charges on your credit cards." I refused to say this. I explained to them many times that this is not correct and the media is not correct.

Because it was only my third week, I was supposed to still be following my script verbatim. But doing it my way I was making five to seven sales a day, even though the quota is three a day (the service is $296). So the boss was monitoring when I did it my way. The boss called me into his office and said he was letting me go. I went back to my cubicle to get my briefcase and my two supervisors were going through my briefcase. They said it was because they wanted to make sure I didn't steal anything. I happened to have the latest issue of *2600* in there (they published one of my letters!), so one of my supervisors held it up and said, "What the fuck is this? You stealing credit card info?" I was so pissed off that I grabbed my briefcase, stuck my mag back in, and walked out the door. To think that just because I read *2600*, just because I defended hackers, I must be a thief.

I feel saddened and hurt that that is the view the public has of us.

Tuxedo Mask

More importantly, you should be proud that you stood up for your convictions. It may feel like shit but what you did took courage and you'll feel better in the end. Hopefully you'll inspire others to do the same and then we may actually get through to some of these thickheads.

Dear 2600:

I have yet to become a subscriber to *2600* (I buy issues with saved change!) but I do buy every issue and it's all right. Just recently I was calling a friend and accidentally dialed the wrong number, so I hung up before letting it ring, and dialed the right number. I talked to him for about 30 minutes and had a nice chat. Immediately after I hung up, the phone rang and I picked it up. The call was from some paranoid person who has *69 service for the sheer purpose of harassing people like me (or so I am convinced). She proceeded to be very rude with me until I told her that I was sorry and promptly hung up on her. Sure, I might not have followed proper phone etiquette (because I hung up before I thought the call had been connected), but I don't think it was any place of her to try to call me back for 30 minutes straight until she got through, just to harass me.

My friends and I, who are very moral and law abiding citizens, have been harassed several times by people who abuse *69. It seems like these people pay the extra just to get *69 so that every time the phone rings they can call back and harass whoever might have called! I have received several nasty calls from these paranoid people, and I'm frankly sick of it. I have a question. If I call someone, accidentally, and then they call me back and harass me about it, how is that different than if they just called me and harassed me? In my opinion, it is still harassment and it is pretty much the same as a prank call to me. I'm sick of paranoid people who abuse their *69 to harass me every time my modem accidentally dials the wrong number because I was in a hurry, etc. Can't people be a little nicer and maybe before they call me back accept the idea that maybe I wasn't trying to do something "evil?"

Zero_Null

*This is exactly the kind of attitude that is fostered by promoting these controversial services. There is no longer such a thing as an honest mistake - everyone is out to get you and you have to be prepared with Caller ID, Call Return, and Call Trace. It's really pretty sad. You can always block your outgoing calls with *67 if you can't get the line itself blocked. (Incidentally, you used the word harass (or a form of it) eight times in a single paragraph. For your records.)*

Facts

Dear 2600:

Re your current issue, the editorial mentions a magazine called *Signal*. I wondered where I saw that name before? It was a magazine issued by the German government during the Nazi period, featuring pictures of victorious German soldiers.

Ehiggins

Dear 2600:

I recently found this out while looking up the number for Microcenter to pick up the new issue of *2600*. I looked at the front of the phone book where they show pictures of things. They had a Caller ID box on there. The number on the Caller ID box was 513-555-2600. What you think? Hackers in the phone company? Or just a guess at numbers?

Lord Mistical

Our agents are everywhere... By the way, we're shocked and appalled that you didn't send us a copy.

Dear 2600:

Is it just me or are the eyes of Janet Reno (15:2) just like the ones of the orangutan (14:2). Could you be saying that Reno is nothing but a monkey when it comes to computers? (The quote on the inside doesn't prove otherwise.)

Louis Blue

Some things are just too frightening to talk about.

Dear 2600:

I recently bought a new "pen and paper Role-Playing Game" from a company called Eden Studios Inc. The name of the game is *Conspiracy X*. I must say it is an excellent game. But that's not the point. The point is this: as I was reading the book, I saw a disturbing picture on page 41. The picture is that of a hacker, sitting at his computer, with a can of Jolt cola and his mouse pad has "2600" written clearly on it. The disturbing part is the fact that the hacker has a bullet hole in his head, and the bullet went straight through his head and shattered the computer screen! Is this picture supposed to be anti-hacker in meaning? And if it is, why do these pro-government types write an RPG about conspiracies? If it's not anti-hacker, then what the hell is it? Did you guys know about it? It does bear your logo.

Vas Hardline

And again, we're shocked and appalled that you didn't send us a copy.

Metrocard Fun

Dear 2600:

I know that there has been a lot of curiosity as to how the MetroCards on the New York subway system work. Well, I have what you might call a social hack, although I haven't had the opportunity to try it yet. Since the new "unlimited" MetroCards have come out (you can ride 30 days for $63), the MTA has encouraged people to share them with family members and friends. But in order to prevent me from passing back my card to someone else right after I enter a station, there is a blackout period which prevents the card holder from

entering the same station twice for 18 minutes. Well, it occurred to me - the MetroCard works on the subway and the bus. What if I was on the bus for more than 18 minutes, walked up to the front of the bus and offered to pay someone's fare with my card? Would the bus driver object? Would transit police storm the bus? It seems like it should be allowable, since I would be "sharing" the card. I hope *2600* readers in New York try this and report back what happens. It should be interesting!

Loggia

Some of us did just such a thing the day the cards became operational. Four of us started swiping people into a subway station the minute the cards became useful. Since each card didn't work for 18 minutes after the last swipe and we timed it evenly between us, we were able to let one person in around every five minutes. The system has since been changed so the time restriction doesn't apply to other stations. We envision gangs of roving youths walking up and down avenues and stopping at each subway station to swipe a bunch of people in. For those who don't want to invest that much time, simply swiping on the way out as well as on the way in will ensure that someone else gets into the system and help make a friendlier city.

Fun Sites

Dear 2600:

After searching for sites on closed systems, I have found some sites where you can make a robot take pictures of classrooms, or make robotic arms look at little gardens, or even make things appear on an electronic sign. By the way, a closed system is where you can send information to a transducer and get a confirmed result, like a computer that turns on a light and then the computer beeps to tell you that the light is on for sure.

The site for controlling the robot is: *http://www.cs.cmu.edu/afs/cs.cmu.edu/Web/People/Xavier/* Xavier is the robot, and he runs on sonar, laser, and a camera to sense his way around the halls at Carnegie-Mellon. You must input your e-mail address to get a picture confirming that he did the task that you asked of him. You can also make Xavier say hi to professors and other things. There are specific times that he can be operated, so be a little crafty.

If you want to see a garden, the site is: *http://www.usc.edu/dept/garden/* The garden picture will pop up right away, and all you have a do is click on an image map. You are able to manipulate a robot arm and choose an area where you want to plant a seed, water it, and make sure it gets enough artificial sunlight. The camera on the robotic arm lets you view your handiwork.

The site for a Remote Access Astronomy Project Remotely Operated Telescope is: *http://www.deepspace.ucsb.edu/rot.htm* This site lets you look into space - it's kinda self explanatory. There is a digital camera located at the top of the Broida Hall, the physics building at UCSB, and it is attached to the back of a computer-controlled Celestron 14" telescope. All you have to do is fill out a form and include some information about where you want the telescope to look. It includes examples for you morons. If you would like some coordinates, try ra: 16h 29m 24s, dec: 26d 41m 00s south, gain: 4, exmc: 6. Both filters remain at 8 (empty). Include a valid e-mail address, so you can get a picture confirming the telescope took pictures. You can use anything for ra and dec but you may have some problems if it's too close to the sun, so try anything above 14:00.

If you want to look at people on the beach, go to: *http://www.fixed.net/beachcam/* You can go look at people on the beach! The photos here are clear and updated every 10 minutes. It's located in Venice Beach, on top of a store that does photo processing, jewelry, and other things. For those of you who care, the store is called Good See Store.

And for the electronic sign, go to: *http://home.netscape.com/people/nitro/sign/* Sometimes the sign gets a little clogged and the phrase you wish to post may be knocked off. Just keep trying. This sign is connected to a Silicon Graphics IRIS machine. It's located at the engineering pit at Netscape, so try to say something profane to the engineers!

There are a few other places I have found, but they are all pretty lame, like viewing a refrigerator and the temperature inside, or talking to a stupid ass cat, or even looking at the number of Cokes in a pop machine.

KRaZy d0k

This letter cost us hours of valuable production time. Educational, though.

Still More FYROM Fun

Dear 2600:

I've read a letter by Christos Parackeyopoulos about the country FYROM which you placed as Macedonia with the abbreviation MAC. I also read your answer which I found rather disturbing (for me at least) and a bit ironic. I guess you don't care how the UN decides each new country's name and you call it with the name you decide. I would like to ask you to change the abbreviation MAC with the correct one, which is FYROM. And as far as the part which says: "Unless going around calling countries names like FYROM is your idea of humor," I would like to inform you that our idea of humor is going around calling countries names like USA.

Varelides Marios
(An angry Greek)

That's actually pretty funny. But the thing is, we call people in our country Americans because it's part of the USA name. Macedonia is part of the FYROM name yet you don't want us to call them Macedonians. You're mad at us for the wrong reason. If the country were called the Former Yugoslav Republic of Idiots, we would call them Idiots but we wouldn't call them FYROI's. We'd really like to know - what do you call those people who live in that place you don't like to say? And keep it clean.

Progress Continued from Page 5

glance at the many forums on the subject reveals that most people don't think the hack itself is a serious matter and that the *Times* had it coming, both for their lack of security and their apparent lack of journalistic integrity. And most everyone began to express an interest in the Kevin Mitnick story. On the www.kevinmitnick.com site (which was linked from the hacked site), our counter went from 13,534 hits the day before the *Times* hack to 62,582 hits the day of the hack and 98,116 the day after! Since then it seems to have leveled off between 20,000 and 30,000 a day but it's clear that a lot of interest was generated and many of those new people have been checking in for updated info. Yes, working within the system is preferable. But we cannot control the way everyone spreads the message, nor should we. When the system doesn't respond to continued injustice, people who have any spirit at all will find some way of getting the word out. The net is a far more level playing field than many of us realize. And the *Times* once again missed an opportunity to get it right by merely vowing to prosecute the hackers to the fullest extent of the law instead of looking at themselves to see what might have spurred this.

But throughout all of this, we cannot forget that Kevin remains in prison day after dreary day. Despite all that has been going on out here in the real world, behind bars things have changed remarkably little. Kevin has yet to even get a bail hearing, let alone bail. His latest appeal for this basic human right was turned down by the United States Supreme Court. He still hasn't been able to see the evidence against him because of the prosecution's irresponsible allegation that his accessing the evidence, only available on computer, would somehow create danger. With nearly 10 gigs of data to go through by his trial date in January, we don't see how it's even remotely possible that his defense team can be adequately prepared by then. That, apparently, is how the system works. Kevin will have no preparation for his defense and be forced to either go into court with a tremendous disadvantage or accept an "offer" from the prosecution which would no doubt keep him in prison for even longer and more important to the prosecution, erode his support network by making him "guilty" in his own words. It's a painful and difficult decision for anyone to have to face. It takes strength to keep up this fight day after day and prison is designed to erode one's strength. The support that people have shown, particularly in recent months, has done much to build Kevin's resolve and to emphasize that maybe things aren't hopeless after all.

No matter what kind of torture/mind games they put him through on the inside, we on the outside must not back down. This has gone on for far too long. Kevin Mitnick deserves to be released *immediately*. It's no longer an issue of what he did. Enough is enough. His continued incarceration for what he was accused of is nothing short of a human rights abuse. We managed to make this clear to Hollywood. Now it's time for Washington.

Please show your support by getting as many "Free Kevin" bumper stickers visible as you can. We're selling them for $1 each with a minimum order of 10. Every penny goes towards Kevin's defense fund. We're donating the cost of printing so nothing will be deducted from your contribution. Make your checks/money orders out to Kevin's grandmother, Reba Vartanian, and mail them to us - 2600 Bumper Stickers, PO Box 752, Middle Island, NY 11953. *Do not make your checks out to 2600!*

You can also show support by grabbing the virtual "Free Kevin" bumper sticker available on the web sites named above and getting it placed on as many sites as you can (with permission, please!). If you're interested in printing out a leaflet and distributing it, you can find a section for downloading them on our sites as well.

More on SIPRnet

by Ex-Eleven

As an open systems geek who makes a living doing network integration along with network security, it makes me smile when my compatriots find weaknesses that I've escalated to network administrators. I'd like to give a big shout out to the Ruiner for his recent article. Sometimes in the course of my job, I get to work on "sensitive" networks. The SIPRnet is an example of this.

To summarize what Ruiner said, SIPRnet is a network primarily composed of Un*x systems that are connected via encrypted links. In his time there was a dial-up modem pool that used Cisco 2511 terminal servers and challenge/response authentification. By and large what he stated is pretty darn accurate, although there have been some changes. We'll get to those shortly.

SIPRnet is a defense network that connects schools and individual hosts that are classified at the secret level. This means that you will find unclassified documents on it (by virtue of being added to a secret host, they become secret) and secret classified documents on the network but you won't find top secret things like plutonium levels within warheads or launch codes. The SIPRnet is managed by DISA (Defense Information Systems Agency) from a bunker inside a mountain. For those of you who care, the bunker is at Ft. Detrick in Frederick, MD.

The dial-up ports have been eliminated to the best of my knowledge and they certainly are not endorsed or supported by SIPRnet network operations. Connectivity is provided via Frame Relay connections starting at 56k and working their way up. Line provisioning is done through GTE government systems. No surprise there. The connectivity is done as follows: The line is fed into a standard Motorola CSU/DSU which connects to the encryption unit (probably triple DES). The CSU/DSU side of the crypto is known as the black side. The router side is known as the red side (because this is the unencrypted side). The router is either a Cisco 2501, 2514, 4500, or 7000 depending on the users' needs.

The cryptography unit is either a KG-84 or a KIV-7. The KG-84 has been manufactured by several different companies including Bendix and Allied Signal. The KIV-7 is manufactured by Allied Signal. Both units are designed and approved by the NSA. When installed initially they are basically dumb boxes, until someone loads the crypto keys that will be used on the link. As I understand it, the keys are loaded via a *paper tape*, although I haven't been able to find this out for sure. I do know that it's something like that but cannot find out since I am not a cleared individual. I know that the crypto devices change their key throughout their connections via something called an OTAR. OTAR stands for Over The Air Rekey. They also have to have a device called a CIK plugged in to be operational. The CIK is a Crypto Ignition Key that looks like a small two-sided plastic comb. When the crypto device is separate from the CIK, it is considered sensitive but not classified. The opposite also applies.

The hosts that are attached to the network have to be secured to at least a C-2 level. Security levels are tested by a SIPRnet tiger team out of Virginia. The exception to this rule though is that there are some NT boxes attached to this network. As you all know, NT is not C-2 unless it doesn't have a network card or floppy drive (go figure).

SIPRnet holds a lot of opportunities for those who have the skills to get access. Perhaps someone on the inside can give us more details.

ＦＡＸ送信状

送信元　会社名
部署名
役職名
名前　様

発信元　会社名
郵便番号　〒
本社

TEL
FAX
部署名
名前

ページ数 全1枚　本紙を含め全1枚

拝啓　貴社ますますご盛栄のこととお慶び申しあげます。平素は格別のお引き立てを賜り厚くお礼申しあげます。
下記のとおりお申し込み申しあげますので、ご査収の上、宜しくお取りはからいくださいますようお願い申しあげます。
敬具

I have a complaint! 2600.com

Fuck you 2600.com

Ada 2600.com

Wannabee 2600.com

all-elbows 2600.com

"JEDGAR" joe@ff.ij4u.or.jp

by FORTRAN MAN!

Do you have a message for us? No matter how unintelligible or insane you happen to be, our fax lines are always open for you. (516) 474-2677. Country code 1.

MARKET PLACE

☏ ☏ ☏ For Sale ☏ ☏ ☏

ATTENTION HACKERS AND PHREAKERS. For a catalog of plans, kits, and assembled electronic "tools" including the RED BOX, SLOT MACHINE MANIPULATORS, SURVEILLANCE, RADAR JAMMERS, LOCK PICKING, and many other hard to find equipment, send $1 to M. Smith 03, 1616 Shipyard Blvd. #287, Wilmington, NC 28412 or visit http://www.hackershomepage.com.

INFORMATION IS POWER! Get our catalog of informational manuals, programs, files, books, newsletters and videos for only $1 (S&H). Our products cover information on hacking, phreaking, cracking, electronics, virii, anarchy and the Internet. Legit and recognized world-wide. Send your $1 US to: SotMESC, Box 573, Long Beach, MS 39560.

WIRETAPPING, cellular monitoring, electronic surveillance, photographs, frequencies, equipment sources. 16 page pictorial of the equipment used in a real life countermeasures sweep. Never before published information in THE PHONE BOOK by M L Shannon. ISBN 0 87364 972-9. 8 1/2 x 11 paperback, 253 pages. Autographed copy $43 postpaid as follows: check or money order payable to Lysias Press for $38, second check or money order for $5 payable to Reba Vartanian to be forwarded to 2600 for the Kevin Mitnick defense fund. Lysias Press, PO Box 192171, San Francisco, CA 94119-2171. Also available from Paladin Press, PO Box 1307, Boulder, CO 80307 and by special order from Barnes and Noble.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; FORBIDDEN SUBJECTS CD-ROM (330mb of hacking files) $17 ppd; DISAPPEARING INK FORMULAS - safely write memos, love letters or nasty notes. Fade time is adjustable. $5 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

PABLO'S ONLINE: http://www.pablos.com. Not just the same old cheap pick sets and maybe a pick gun. We have access to the bleeding edge locksmithing tools, from code books to safe penetration to '99 model auto entry! We specialize in special orders. Stop getting gouged/ripped off by lamer spy shops, and let us equip you with the latest and greatest in the trade. Also, switchblades, exotic weaponry, non-lethal self-defense, and more. Your BEST PRICE beat, and YOUR SATISFACTION GUARANTEED. Serving professionals since 1985.

HACK THE RADIO: Hobby Broadcasting magazine covers DIY broadcasting of all types: AM, FM, shortwave, TV, and the Internet. It includes how-to articles about equipment, station operation and programming, enforcement, and much more. For a sample, send $5 U.S. ($6 Canada or $5 international). A subscription (4 quarterly issues) is $12 in the U.S. Hobby Broadcasting, PO Box 642, Mont Alto, PA 17237.

OFFERING SIX VIRUSES/VERI which can automatically knock down DOS and Windows 3.1 operating systems at the victim's command to open Windows. Easily loaded, recurrently destructive, and undetectable via all virus detection and cleansing programs with which I am familiar. Well-tested, relatively simple, and designed with stealth and victim behavior in mind. Well written instructions, documentation, and antidote programs are included. $5 even TOTAL! Cash, money orders, and checks accepted. Sorry, no foreign orders. Provided on seven 1.44 MB, 3.5" floppy disks which can be freely copied. They make great gifts! Orders are promptly mailed out "priority" (USPS). Satisfaction guaranteed or you have a bad attitude! The Omega Man, 239 Lexington Rd., Elgin, TX 78621-1645, omegaman4@juno.com.

BROADEN YOUR MIND! I am selling the following information for cheap. Set up Windows 3.xx with multiple configurations. Complete code and instructions to give each user different wallpaper, screen savers, even screen resolutions! Much more! Only $4.00. How to change the startup graphic in all Windows versions. Bonus: how to change Win 95/98 exit screen. All for only $2.00. Pamphlet on how to hide files, e-mail, etc. in a graphic picture. Can store files up to 200k. Requires programming knowledge. Only $2.00. Send cash, check, or money order (preferred, for fastest service) to: John D. Lord, PO Box 488, Boonville, IN 47601.

☏ ☏ ☏ Help Wanted ☏ ☏ ☏

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

LUCRATIVE JOINT VENTURE. "Top Gun" hacker or surveillance expert needed. Call in complete confidence: Ross (612) 306-1245.

SEEKING HELP on how to identify unauthorized duplications of computer software programs by corporate entities. Possible reward for those who can help. Please respond to: Martin Drost, 4940 W. Dempster, Skokie, IL 60077.

☏ ☏ ☏ Wanted ☏ ☏ ☏

DONATIONS DESPERATELY NEEDED to help stock prison library with computer manuals, magazines, and other computer related material. The administration of this facility refuses to use funds from the library budget to purchase such materials because, as one official said, "Convicts aren't smart enough to operate a computer, nor should they be." The admin did state, however, that I'm free to donate computer related material to the library myself, if I want. If you would like to help, please send books, magazines, or money orders (no checks) to: Jeffery Kock #256860, Ionia Maximum Facility, 1576 Bluewater Hwy, Ionia, MI 48846. All books and magazines must come directly from the publisher. Personal correspondence also welcome and appreciated.

WANTED: Heathkit ID-4001 digital weather computer (working). Also wanted: Heathkit: ID-1890, ID-1990, ID-2090. Does anyone have, or know where one can obtain, a TELEPHONE-LINE POWERED MINIATURE TOUCH TONE TELEPHONE DIGIT LOGGER which will hold in memory, preferably non-volatile, all digits dialed to the extent of at least 75 ten-digit telephone numbers? Contact: WANTED, PO Box 11562 (tn), St. Clt, Missouri 63135.

WE WANT TO BUY DATABASES. We will purchase any public or private database that contains name (or company name) / address / telephone number / date of birth / ssn, etc. or any combination of the above - i.e., driver licenses, motor vehicles, voter registrations, criminal records, corporate records, real property, UCCs, etc. Foreign databases also purchased. Immediate cash paid. Send details to: Mr. Data, POB 155, Midwood Station, Brooklyn, NY 11230.

DO YOU NEED NUMBERS? I want interesting toll-free 800/888 phone numbers such as ANI's, CNA's, PBX's, voice systems, computers, weird numbers, or anything else. I will give you TWO numbers from my collection for every ONE number you send me. Please e-mail all numbers to: onder101@juno.com.

☏ ☏ ☏ Services ☏ ☏ ☏

INFORMATION ARCHIVES. Odd manuals, source codes, etc. $2 + one 32 cent stamp for catalog. NEW: Find anything about anyone! Just send us all the information you have on the person in question and what information you would like to learn for a FREE cost estimate. Information Archives, J. Olsommer, PO Box 222, Lakeville, PA 18438.

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Jr., Attorney at Law, at (334) 265-6002 or cybercrime@dmorrow.com. Extensive computer and legal background.

☏ ☏ ☏ Personal ☏ ☏ ☏

HELP! THIS IS AN SOS MESSAGE. 2600 readers sought as pen pals by computer illiterate prisoner. I seek to discuss "collective thought" possibilities that are financially orientated. Pyramid this message on any anarchy orientated bulletin boards. Thanks. Purcell Bronson, AF8151, Drawer K, Dallas, PA 18612.

BOYCOTT BRAZIL is requesting your continued assistance in contacting PURCHASING AGENTS, state and municipalities, to adopt "Selective Purchasing Ordinances," prohibiting the purchasing of goods and services from any person doing business with Brazil. Purchasing agents for your town should be listed within your town's web site, listed on www.city.net or www.municourt.org. Examples of "Selective Purchasing Ordinances" can be reviewed within the "Free Burma Coalition" web site. Thanking 2600 staff, subscribers, and friends for your continued help in informing the WORLD as to my torture, denial of due process, and forced brain control implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site: http://members.aol.com/BrazilBoycot.

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Winter issue: 12/1/98.

MEETINGS MEETINGS MEETINGS MEETINGS MEETINGS MEETINGS MEETINGS MEETINGS

UNITED STATES

Alabama

Birmingham: Riverchase Galleria Food Court by the payphones next to Wendy's. 7 pm.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Sacramento: Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9544 - bypass the carrier.

San Diego: Cyberia Cafe on Regents Road (Vons Shopping Mall).

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Connecticut

Milford: The Post Mall by Time-Out.

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Pompano Square Mall (SW corner of US 1 and Copans Rd.) on the food court.

Ft. Myers: At the cafe in Barnes and Noble.

Miami: Dadeland Mall on the raised seating section in the food court.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 895-9708; 895-6044, 5055.

Pensacola: Cordova Mall, food court, tables near ATM. 5:30 pm.

Georgia

Atlanta: Lenox Mall food court.

Illinois

Chicago: La Piazza Cafe at 3545 North Broadway.

Kansas

Kansas City: Food Court at the Oak Park Mall in Overland Park.

Kentucky

Louisville: St. Matthews Mall Food Court.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8777 - good luck getting around the carrier.

Maine

Portland: Maine Mall by the bench at the food court door.

Massachusetts

Boston: Prudential Center Plaza Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Northampton: Javaher Cafe at 241 Main Street.

Michigan

Ann Arbor: Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Missouri

St. Louis: Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Nebraska

Omaha: Oak View Mall Barnes and Noble, 5:30 pm.

Nevada

Reno: Meadow Wood Mall, Palms food court by Sbarro, 3-9 pm.

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court.

New Mexico

Albuquerque: Winrock Mall Food Court, near payphones on the lower level between the fountain and arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

New York

Buffalo: Eastern Hills Mall (Clarence) by lockers near food court.

New York: Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Rochester: Marketplace Mall food court, 6 pm.

North Carolina

Charlotte: South Park Mall, raised area of the food court.

Raleigh: Crabtree Valley Mall, food court.

Ohio

Akron: Arabica Cafe on W. Main St.

Cleveland: Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus: Convention Center, first level near the payphones with red seats.

Oklahoma

Oklahoma City: Shepard Mall, at the benches next to Subway and across from the payphones. Payphone numbers: (405) 942-9077, 9228, 9161, 9456.

Oregon

McMinnville: Union Block, 403 NE 3rd St.

Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9119, 9779, 9799; 387-9751.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Mall/Chase Galleria in the food court.

Nashville: Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Ft. Worth: North East Mall, food court, Loop 820 @ Bedford Euless Rd. 6 pm.

Houston: Food court under the stairs in Galleria 2, next to McDonalds.

San Antonio: North Star Mall food court.

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Milwaukee: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Cafe Fellini, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: At the Groenplaats at the payphones closest to the cathedral.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

Edmonton: Sidetrack Cafe, 10333 112 Street. 6 pm.

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.

Hull: In the Old Grey Mare pub, opposite the University of Hull. 7 pm.

Leeds: Leeds City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Piccadilly Circus) next to VR machines. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

Paris: Place d'Italie IRIS, in front of the Grand Ecran Cinema. 6-7 pm.

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

IRELAND

Dublin: Phone boxes opposite Stephen's Green Shopping Centre.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

POLAND

Stargard Szczecinski: Art Caffe

RUSSIA

Moscow: Burger Queen cafe near TR/TASS (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nikitskie Vorota.

SCOTLAND

Aberdeen: Outside Marks & Spencers, next to the Grampian Transport kiosk.

SOUTH AFRICA

Cape Town: At the "Mississippi Detour".

Johannesburg: Sandton food court.

SPAIN

Granada: Cibertece Granada in Pza. Einstein near the Campus de Fuentenueva.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

Don't Panic

It's safe to subscribe to 2600. We know a lot of you were afraid that we would disappear and take your money with us. Since we announced our financial problems last year, many of you haven't renewed your subscriptions and have instead gone to the newsstands. Since our problems are now behind us, even the most paranoid people no longer have anything to worry about. Of course, there's the possibility of your name being tracked by all kinds of monitoring agencies. But did you ever think of the risks of not subscribing? You could get hit by a bus crossing the street on the way to the bookstore or get involved in one of the many fights to the death that occur over the last issue on the stands. And those same monitoring agencies will find out what you bought anyway. So play it safe. Have 2600 delivered to the relative safety of your home or office at the same price we've had since 1991!

Name: ______________________ Amt. Enclosed: ________

Address: ______________________ Apt. #: ________

City: ______________________ State: ________ Zip: ________

Individual Subscription

O 1 Year - $21 O 2 Years - $38 O 3 Years - $54

Corporate Subscription

O 1 Year - $50 O 2 Years - $90 O 3 Years - $125

Overseas Subscription

O 1 Year, Individual - $30 O 1 Year, Corporate - $65

Lifetime Subscription

O $260

Photocopy this page, fill it out, and send it to:

2600 Subscriptions, PO Box 752, Middle Island, NY 11953